This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

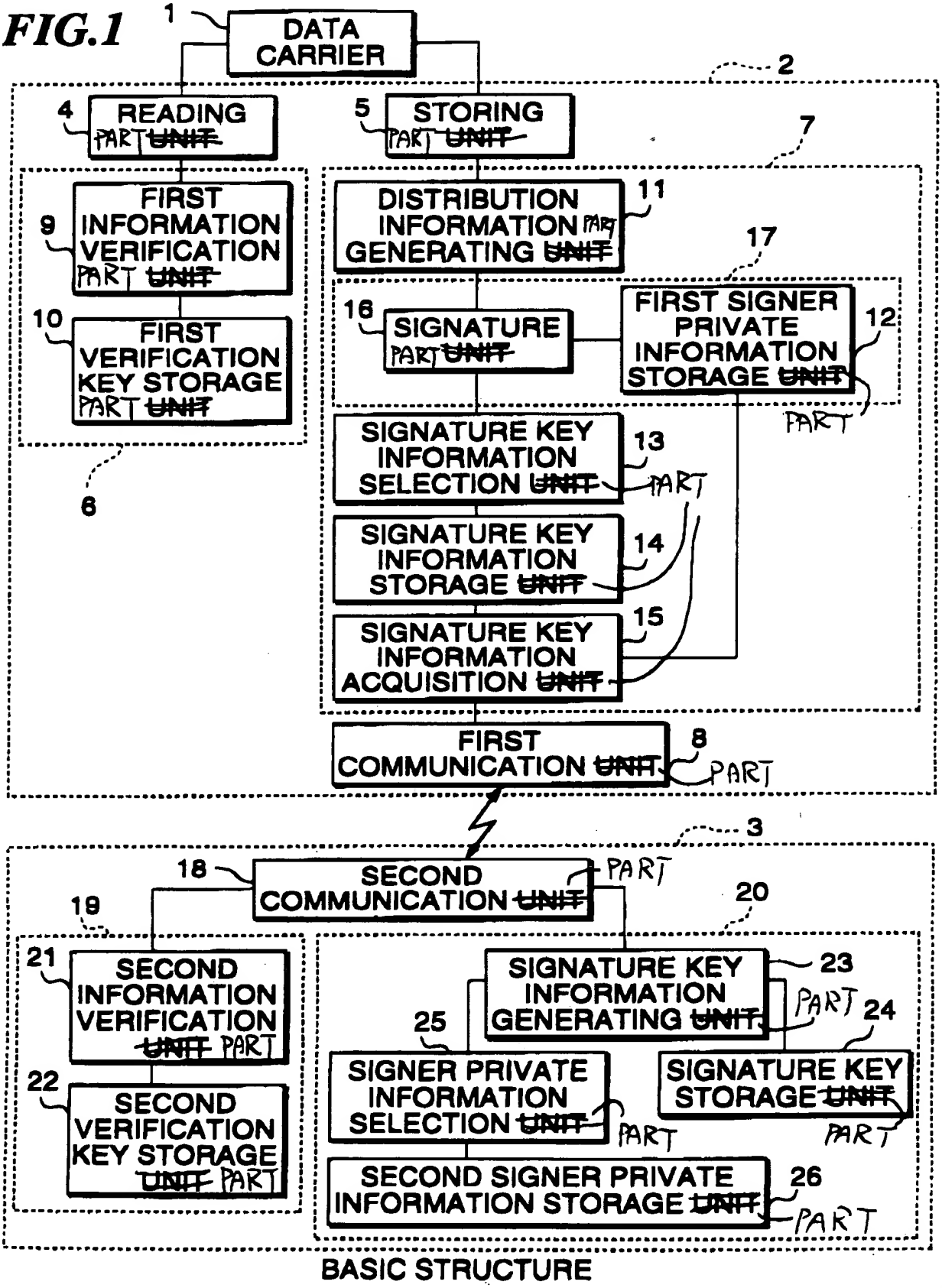
Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

FIG.1



BASIC STRUCTURE

FIG.2

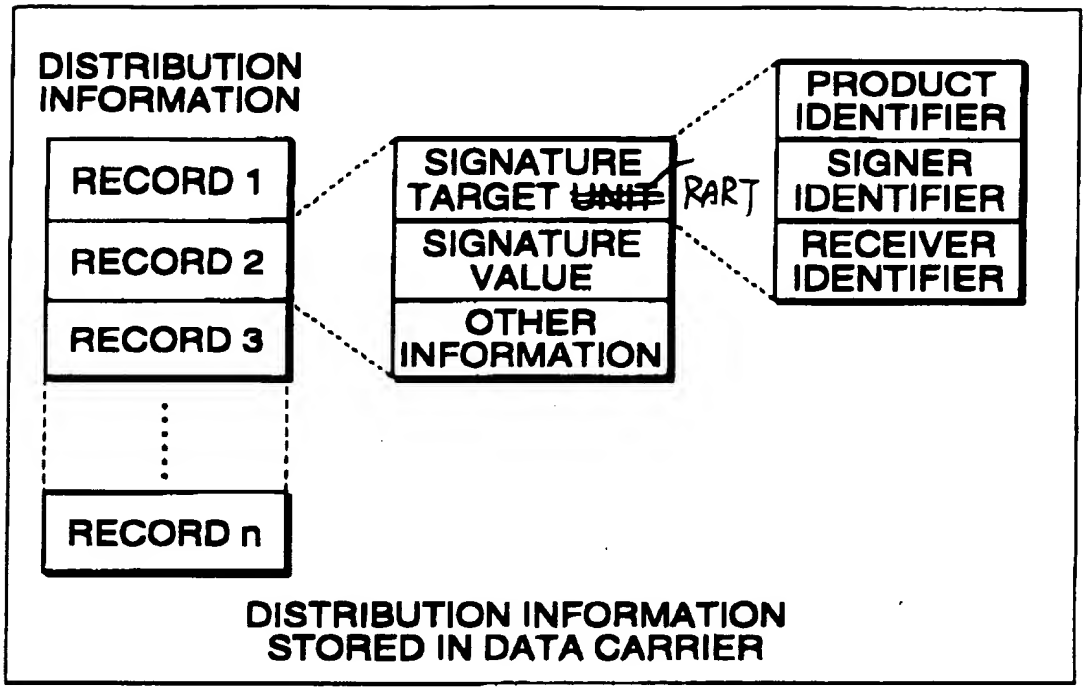
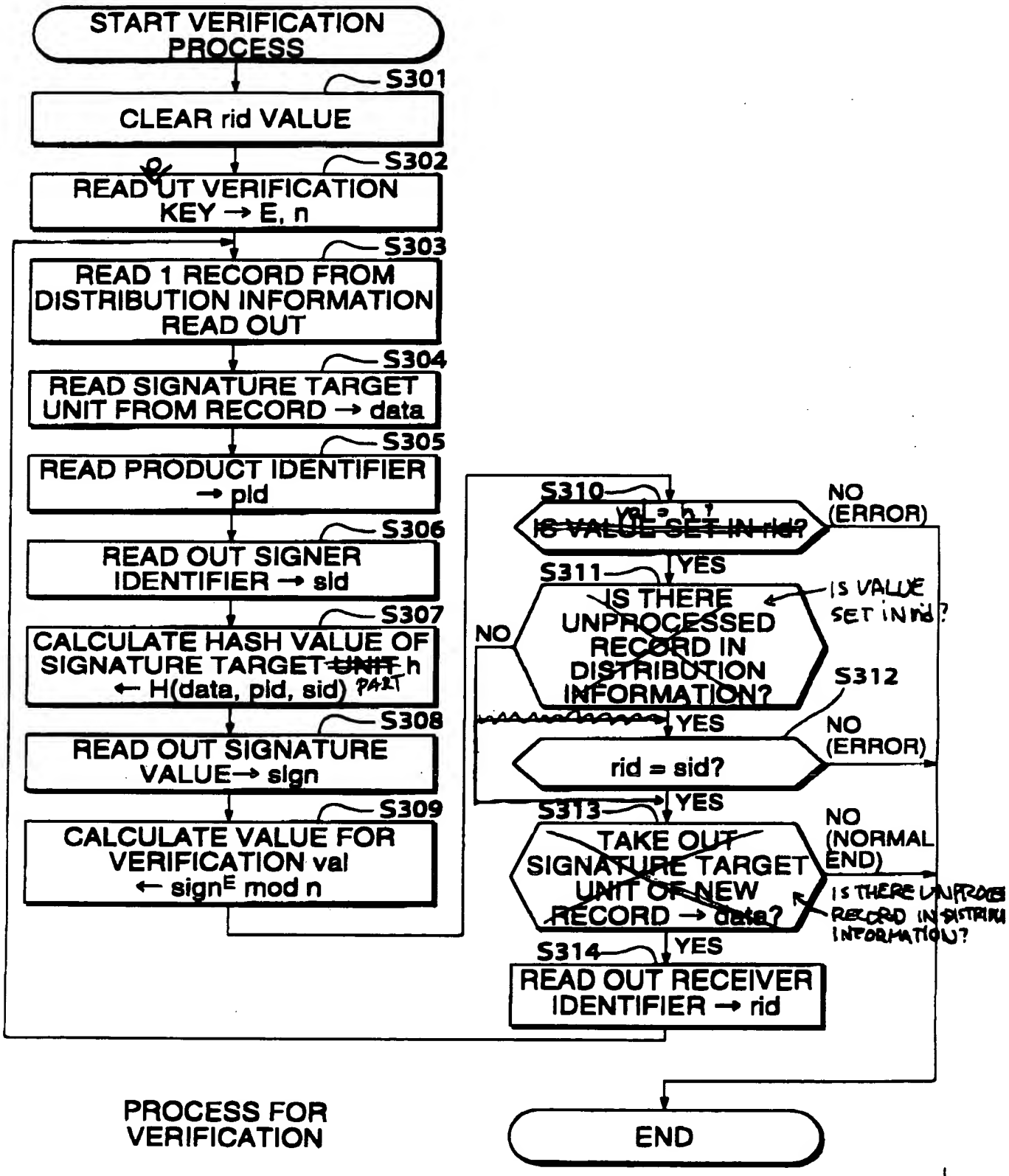

DISTRIBUTION INFORMATION
RECORD 1
RECORD 2
RECORD 3
RECORD n
SIGNATURE TARGET UNIT
PART
SIGNATURE VALUE
OTHER INFORMATION
PRODUCT IDENTIFIER
SIGNER IDENTIFIER
RECEIVER IDENTIFIER
DISTRIBUTION INFORMATION STORED IN DATA CARRIER

FIG.3



PROCESS FOR VERIFICATION

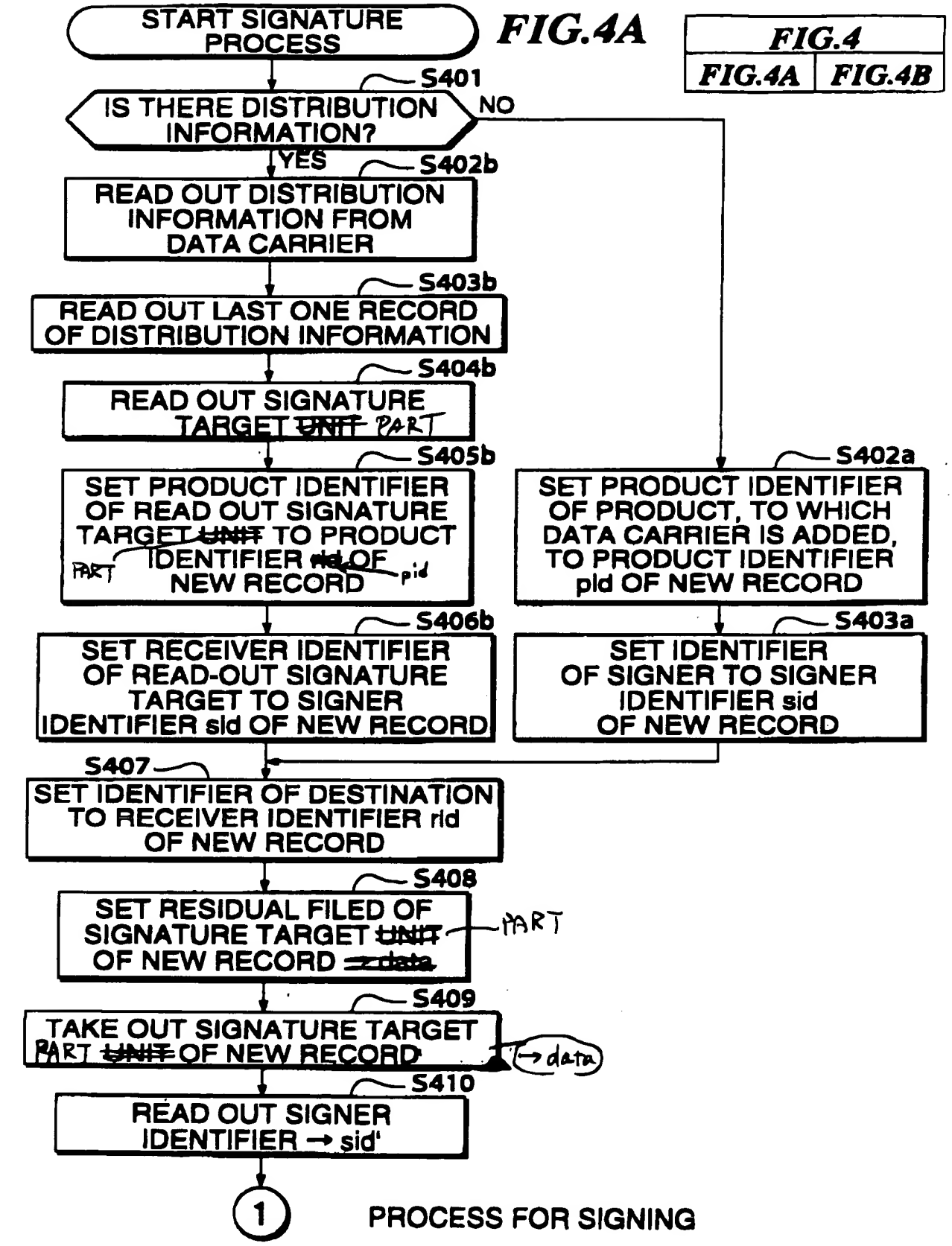
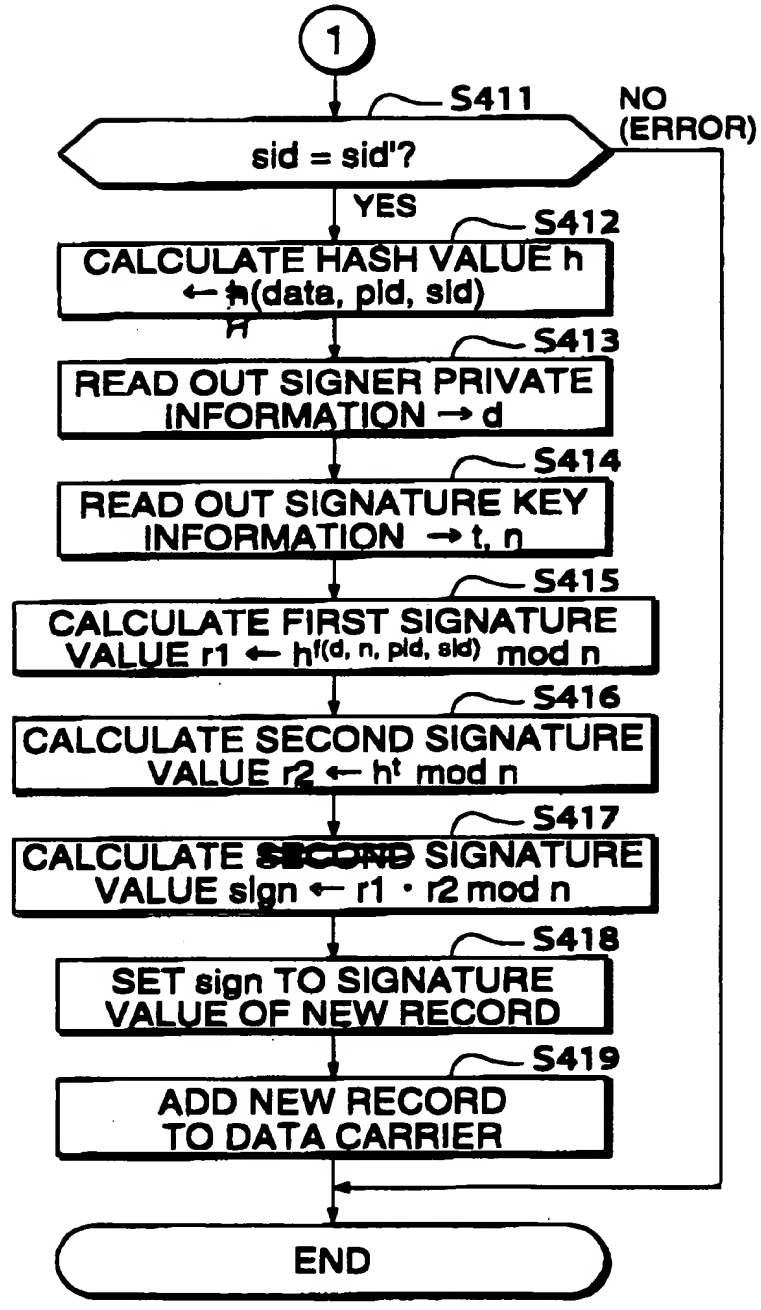


FIG.4A

FIG.4

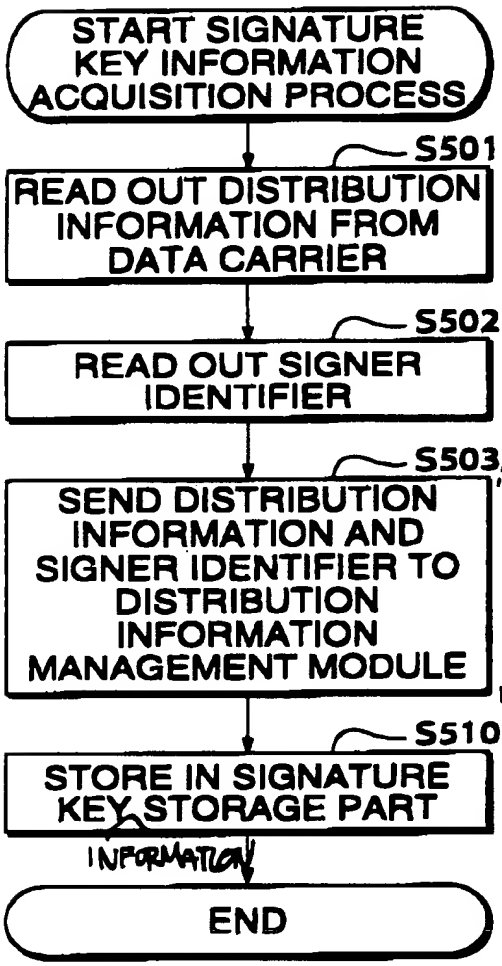
FIG.4A	FIG.4B

FIG.4B



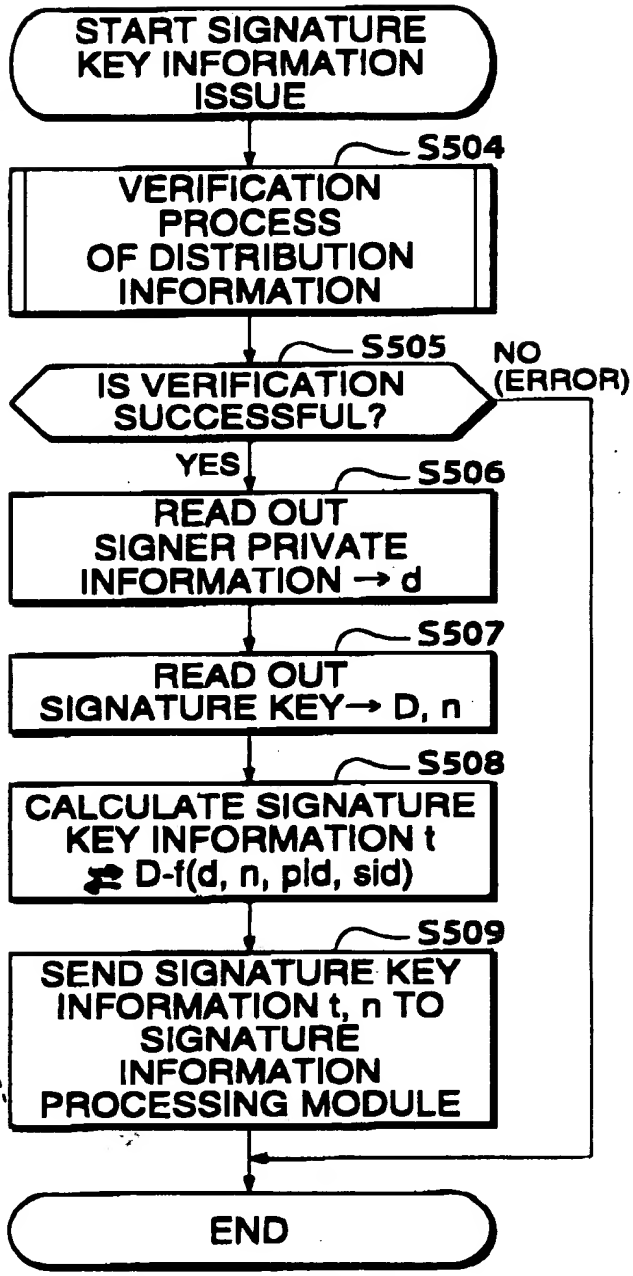
PROCESS FOR SIGNING

FIG.5A



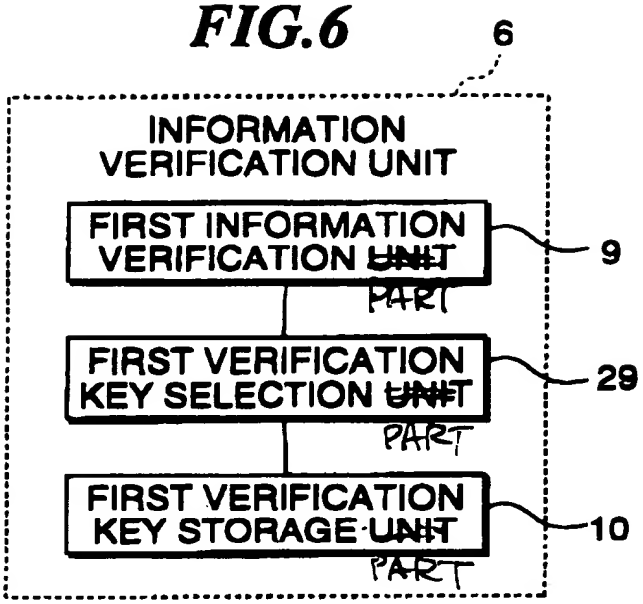
PROCESS FOR SIGNATURE KEY INFORMATION ACQUISITION

FIG.5B



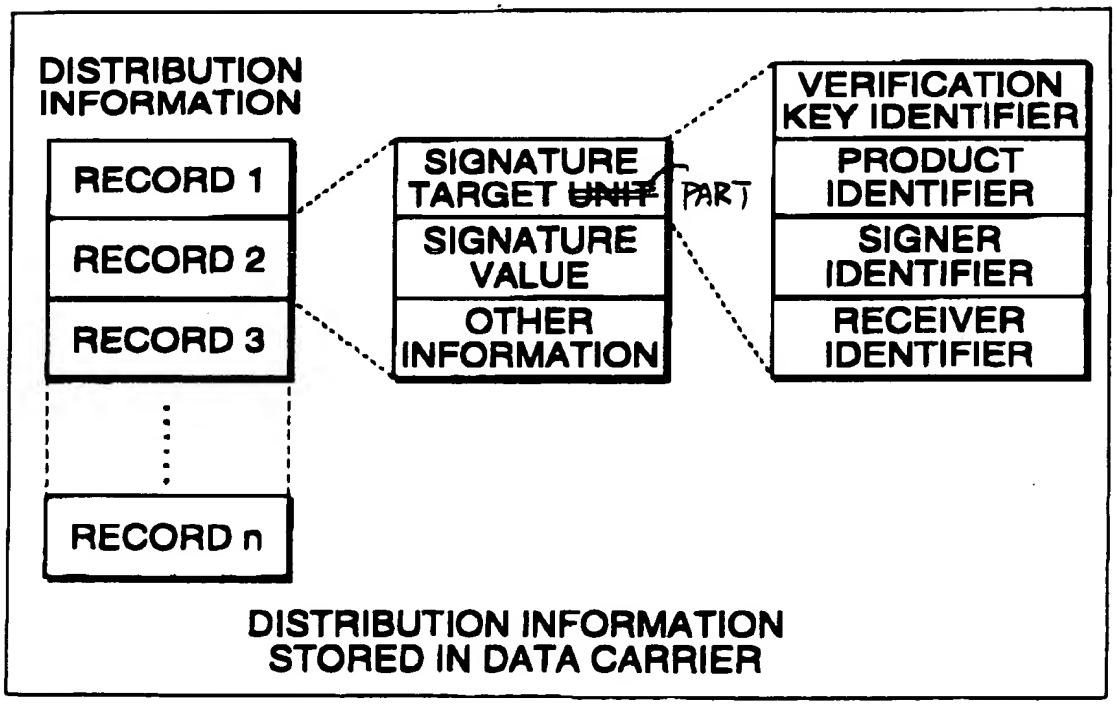
PROCESS FOR SIGNATURE KEY INFORMATION ACQUISITION

FIG.6



INFORMATION VERIFICATION UNIT

FIG.7



DISTRIBUTION INFORMATION STORED IN DATA CARRIER

FIG.8

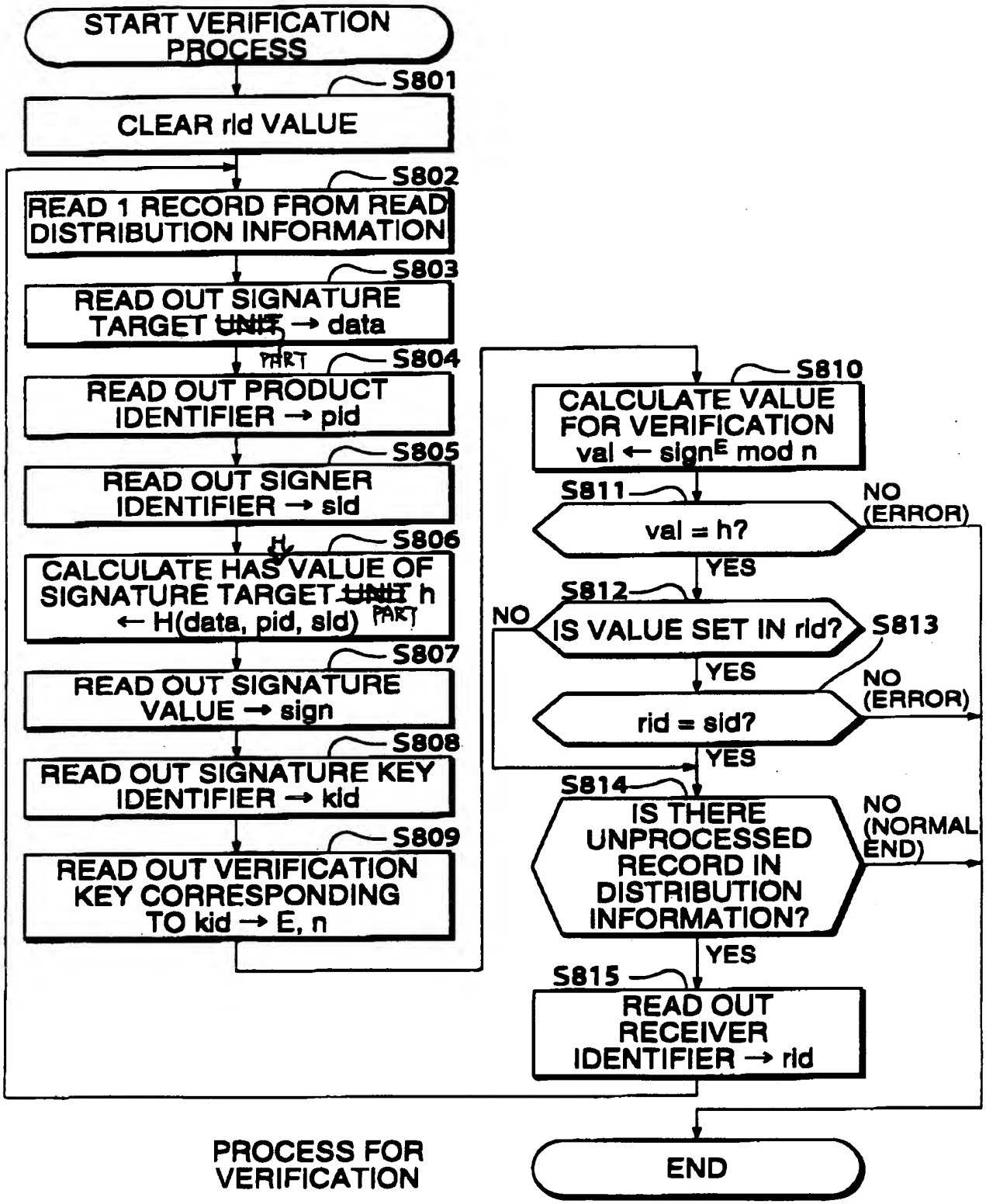

START VERIFICATION PROCESS
S801
CLEAR rid VALUE
S802
READ 1 RECORD FROM READ DISTRIBUTION INFORMATION
S803
READ OUT SIGNATURE TARGET UNIT → data
PART
S804
READ OUT PRODUCT IDENTIFIER → pid
S805
READ OUT SIGNER IDENTIFIER → sid
H
S806
CALCULATE HAS VALUE OF SIGNATURE TARGET UNIT h ← H(data, pid, sid)
PART
S807
READ OUT SIGNATURE VALUE → sign
S808
READ OUT SIGNATURE KEY IDENTIFIER → kid
S809
READ OUT VERIFICATION KEY CORRESPONDING TO kid → E, n
S810
CALCULATE VALUE FOR VERIFICATION val ← sign^E mod n
S811
val = h?
NO (ERROR)
YES
S812
NO
IS VALUE SET IN rid?
S813
YES
NO (ERROR)
rid = sid?
YES
S814
IS THERE UNPROCESSED RECORD IN DISTRIBUTION INFORMATION?
NO (NORMAL END)
YES
S815
READ OUT RECEIVER IDENTIFIER → rid
PROCESS FOR VERIFICATION
END

FIG.9

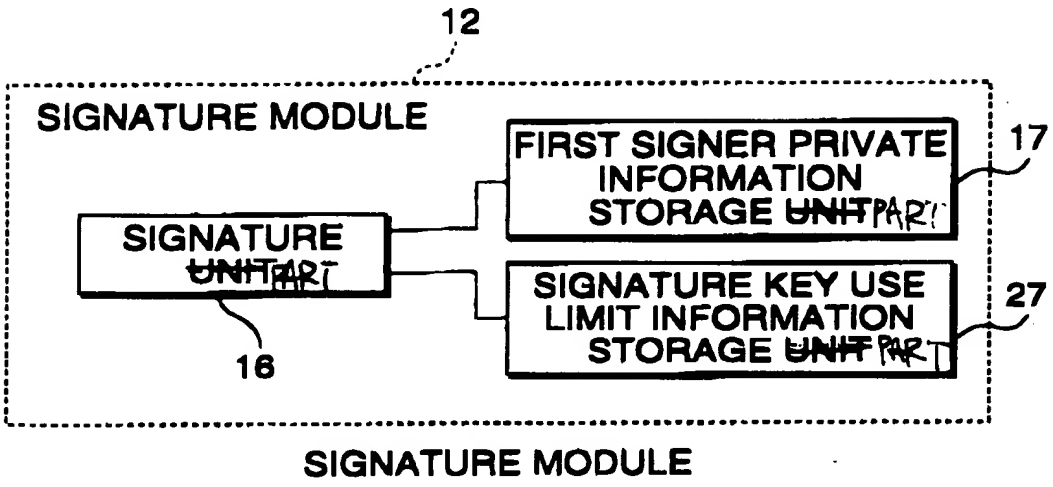
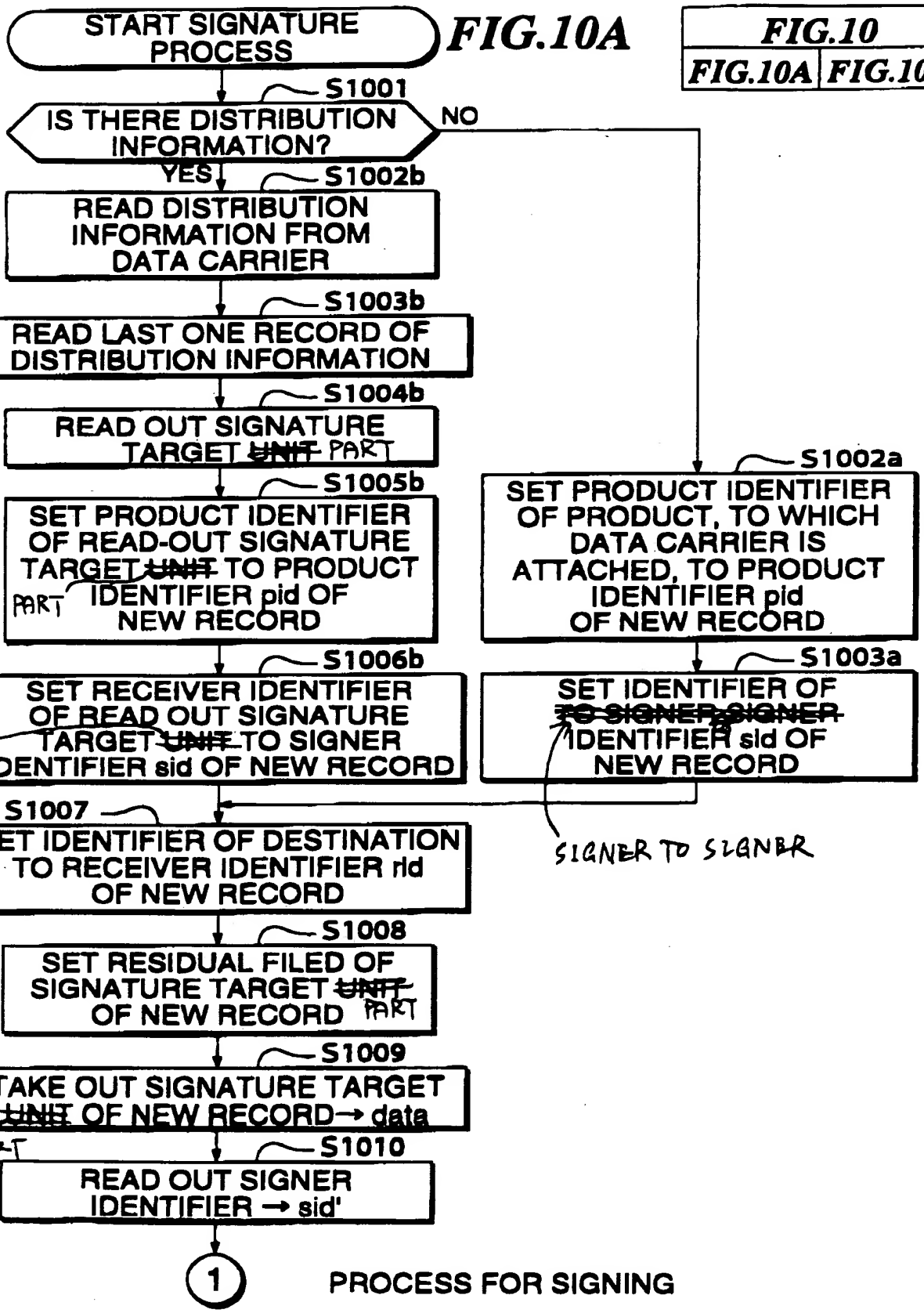

12
SIGNATURE MODULE
FIRST SIGNER PRIVATE INFORMATION STORAGE UNIT PART
17
SIGNATURE UNIT PART
SIGNATURE KEY USE LIMIT INFORMATION STORAGE UNIT PART
27
16
SIGNATURE MODULE

FIG.10

FIG.10A	FIG.10B

FIG.10A



PROCESS FOR SIGNING

FIG.10B

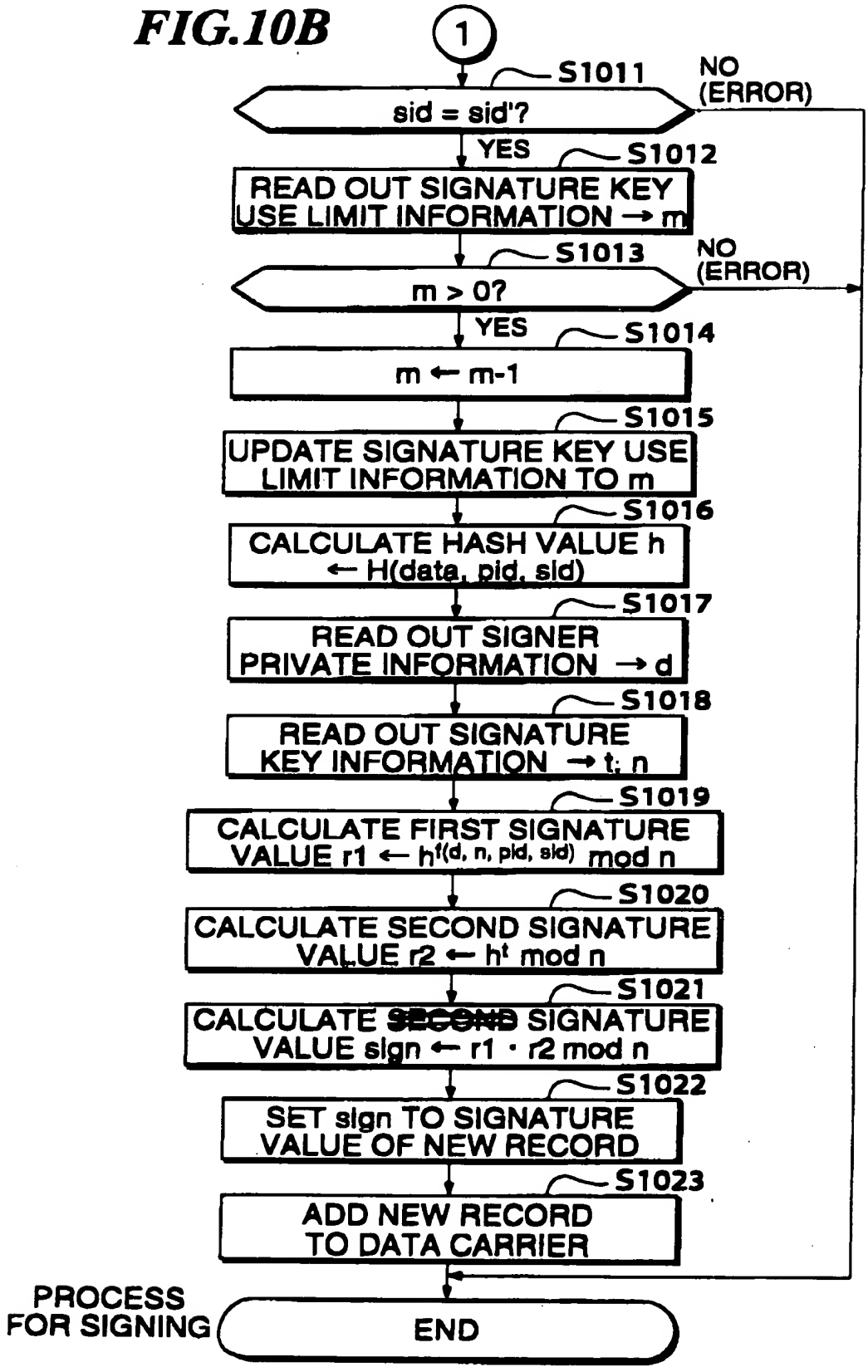

1
S1011
sid = sid'?
NO (ERROR)
YES
S1012
READ OUT SIGNATURE KEY USE LIMIT INFORMATION → m
S1013
m > 0?
NO (ERROR)
YES
S1014
m ← m-1
S1015
UPDATE SIGNATURE KEY USE LIMIT INFORMATION TO m
S1016
CALCULATE HASH VALUE h ← H(data, pid, sid)
S1017
READ OUT SIGNER PRIVATE INFORMATION → d
S1018
READ OUT SIGNATURE KEY INFORMATION → t, n
S1019
CALCULATE FIRST SIGNATURE VALUE r1 ← h^f(d, n, pid, sid) mod n
S1020
CALCULATE SECOND SIGNATURE VALUE r2 ← h^t mod n
S1021
CALCULATE SIGNATURE VALUE sign ← r1 · r2 mod n
S1022
SET sign TO SIGNATURE VALUE OF NEW RECORD
S1023
ADD NEW RECORD TO DATA CARRIER
PROCESS FOR SIGNING
END

FIG.11

FIG.11A	FIG.11B

FIG.11A

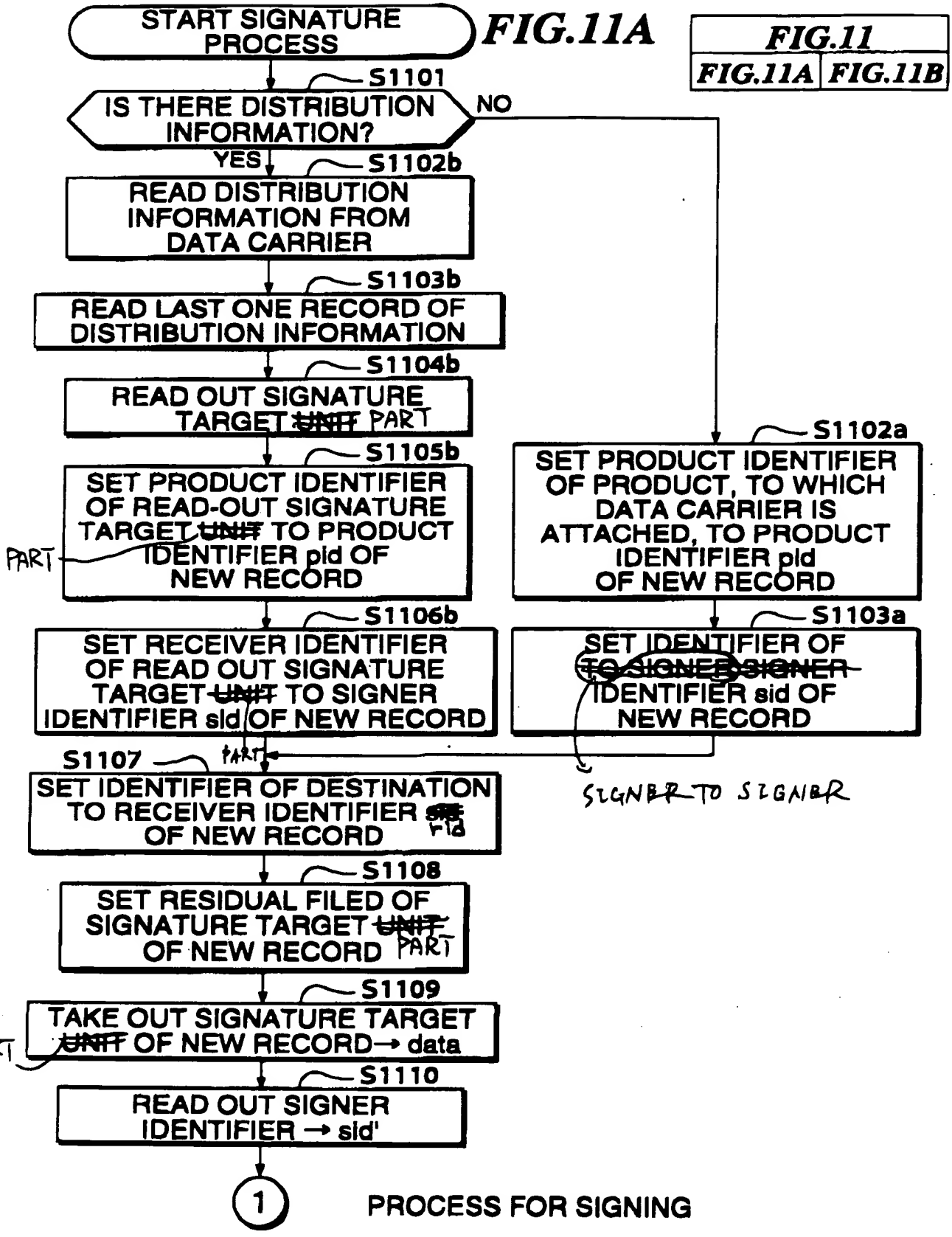
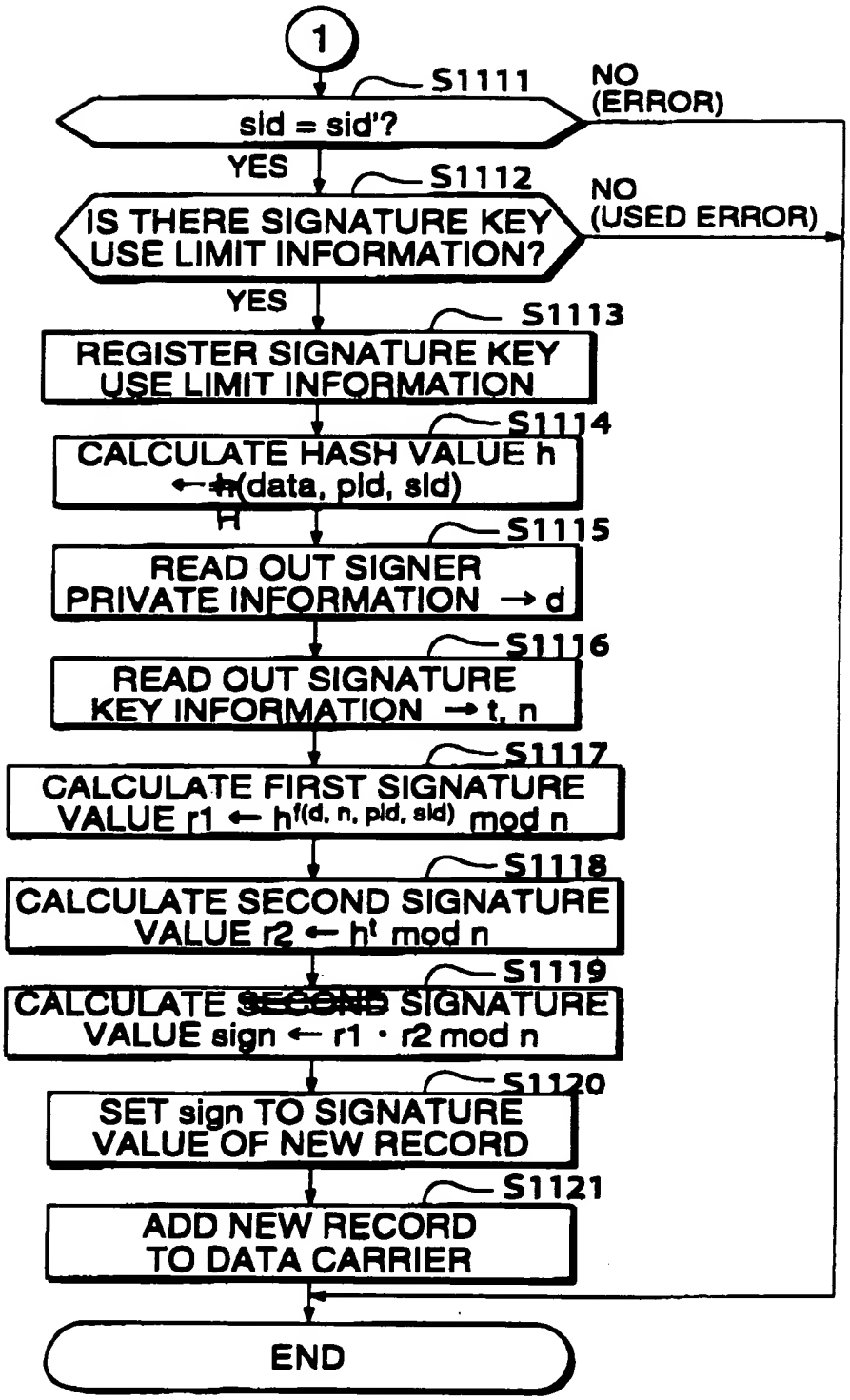
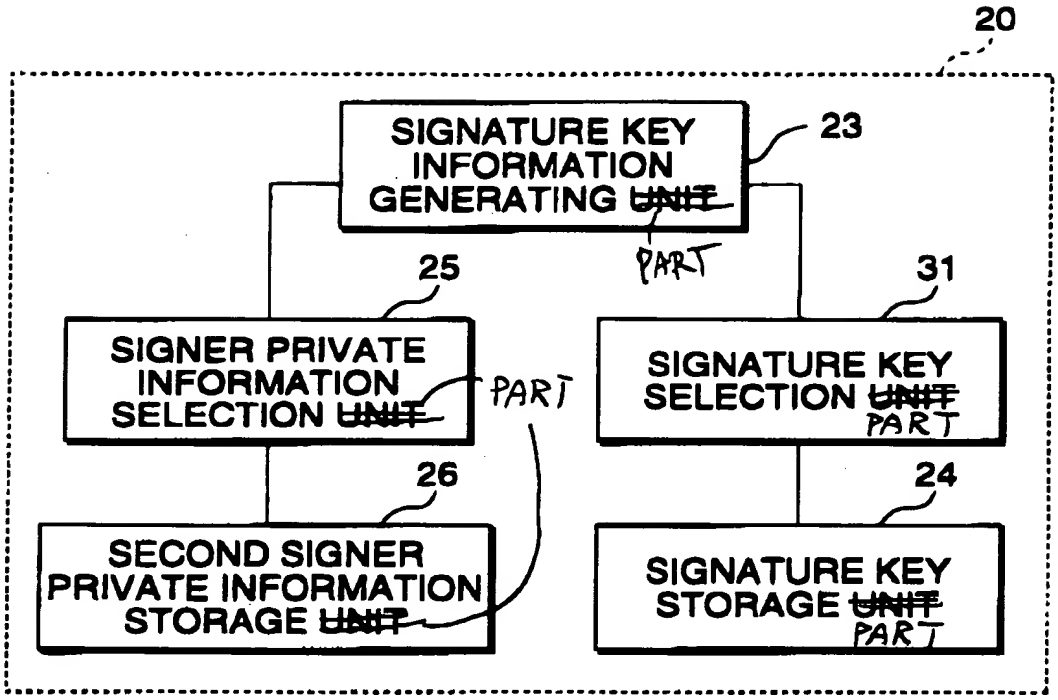


FIG.11B



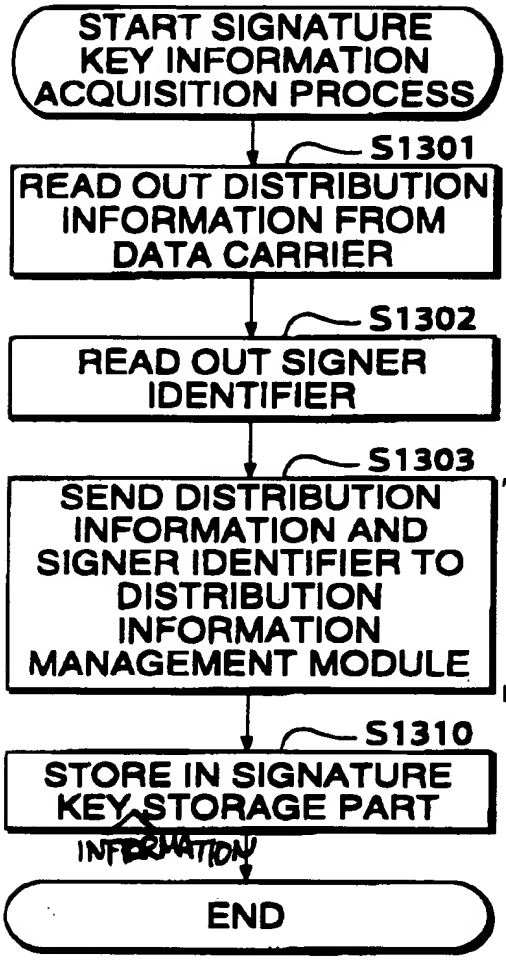
PROCESS FOR SIGNING

FIG.12



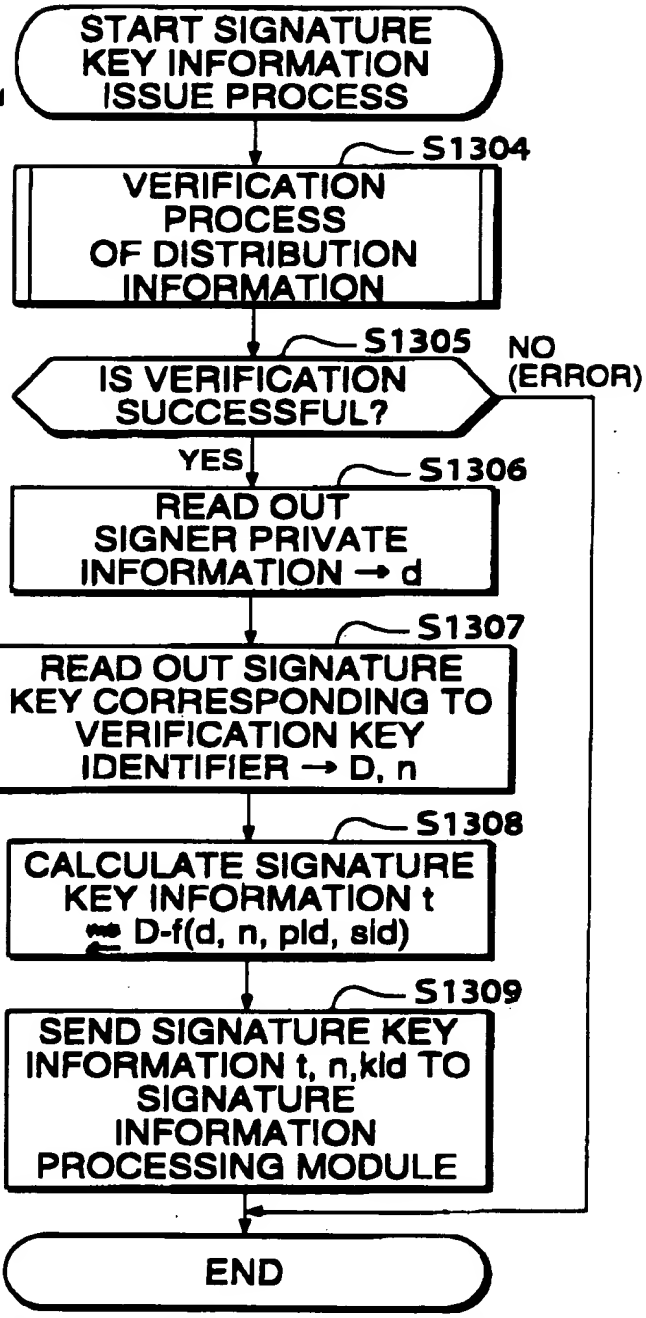
SIGNATURE KEY INFORMATION GENERATING MODULE

FIG.13A



PROCESS FOR SIGNATURE KEY INFORMATION ACQUISITION

FIG.13B



PROCESS FOR SIGNATURE KEY INFORMATION ACQUISITION

FIG.14

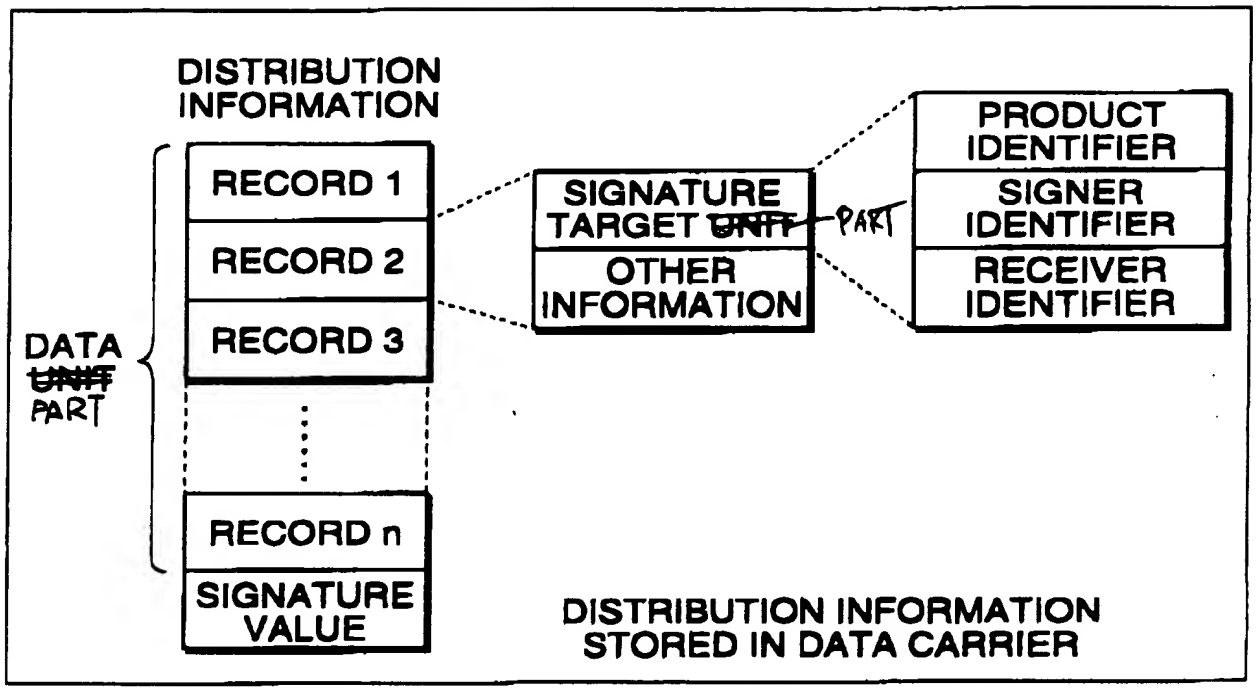

DISTRIBUTION INFORMATION
RECORD 1
RECORD 2
RECORD 3
RECORD n
SIGNATURE VALUE
DATA UNIT PART
SIGNATURE TARGET UNIT PART
OTHER INFORMATION
PRODUCT IDENTIFIER
SIGNER IDENTIFIER
RECEIVER IDENTIFIER
DISTRIBUTION INFORMATION STORED IN DATA CARRIER

FIG.15A

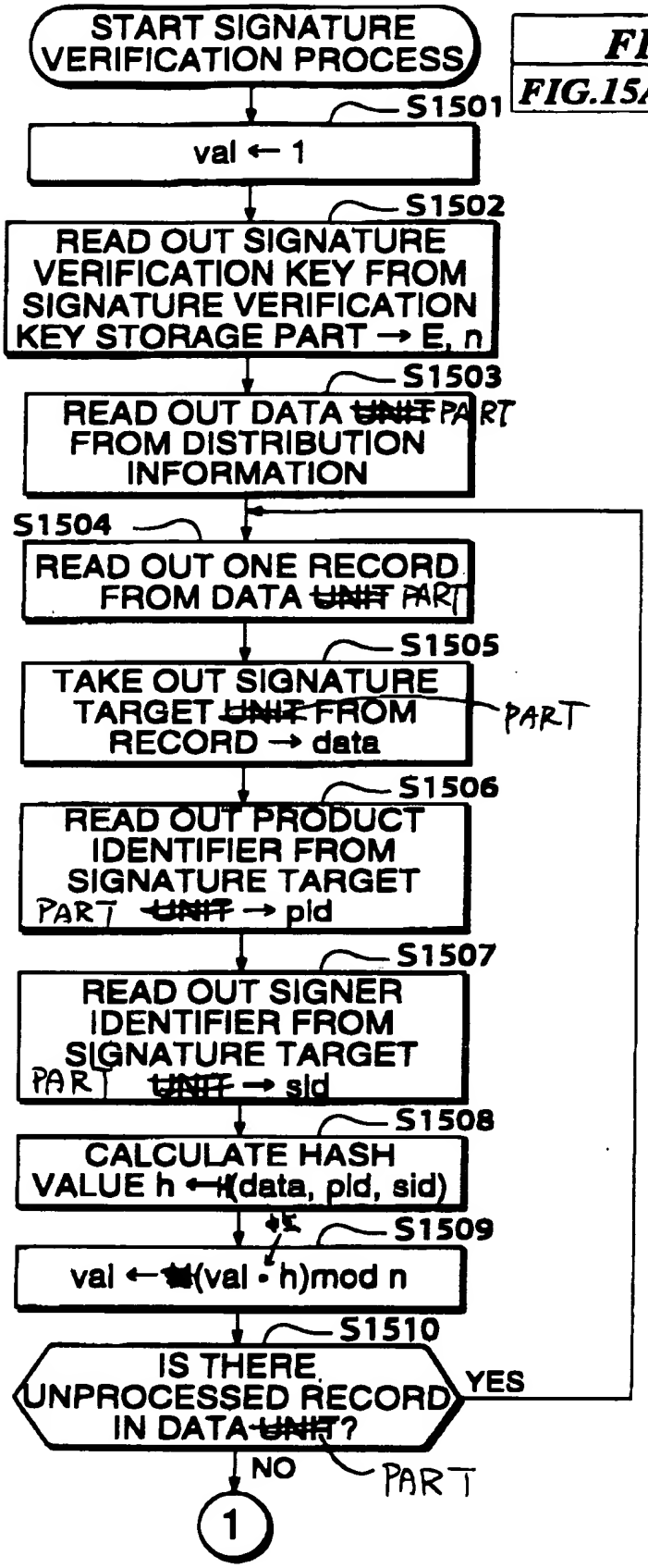
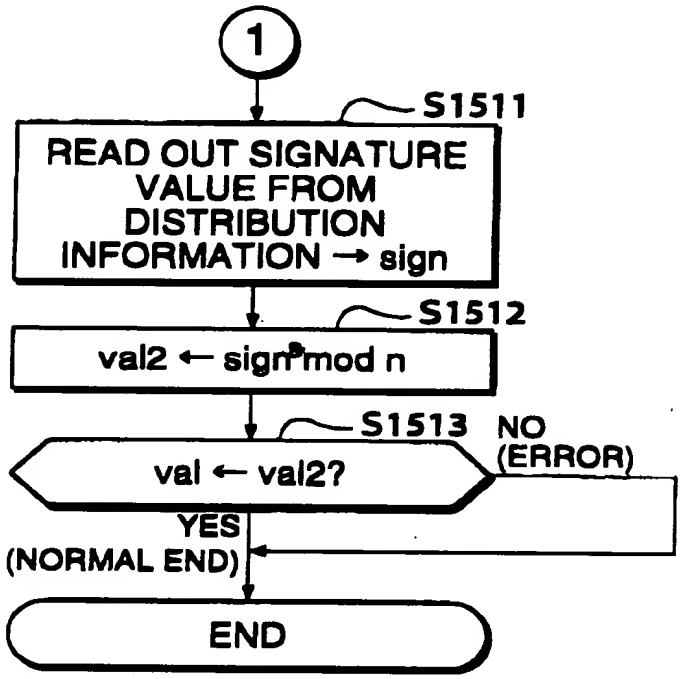


FIG.15

FIG.15A	FIG.15B

SIGNATURE VERIFICATION PROCESSIN THE CASE WHERE THERE IS ONLY ONE SIGNATURE VALUE IN DATA CARRIER

FIG.15B

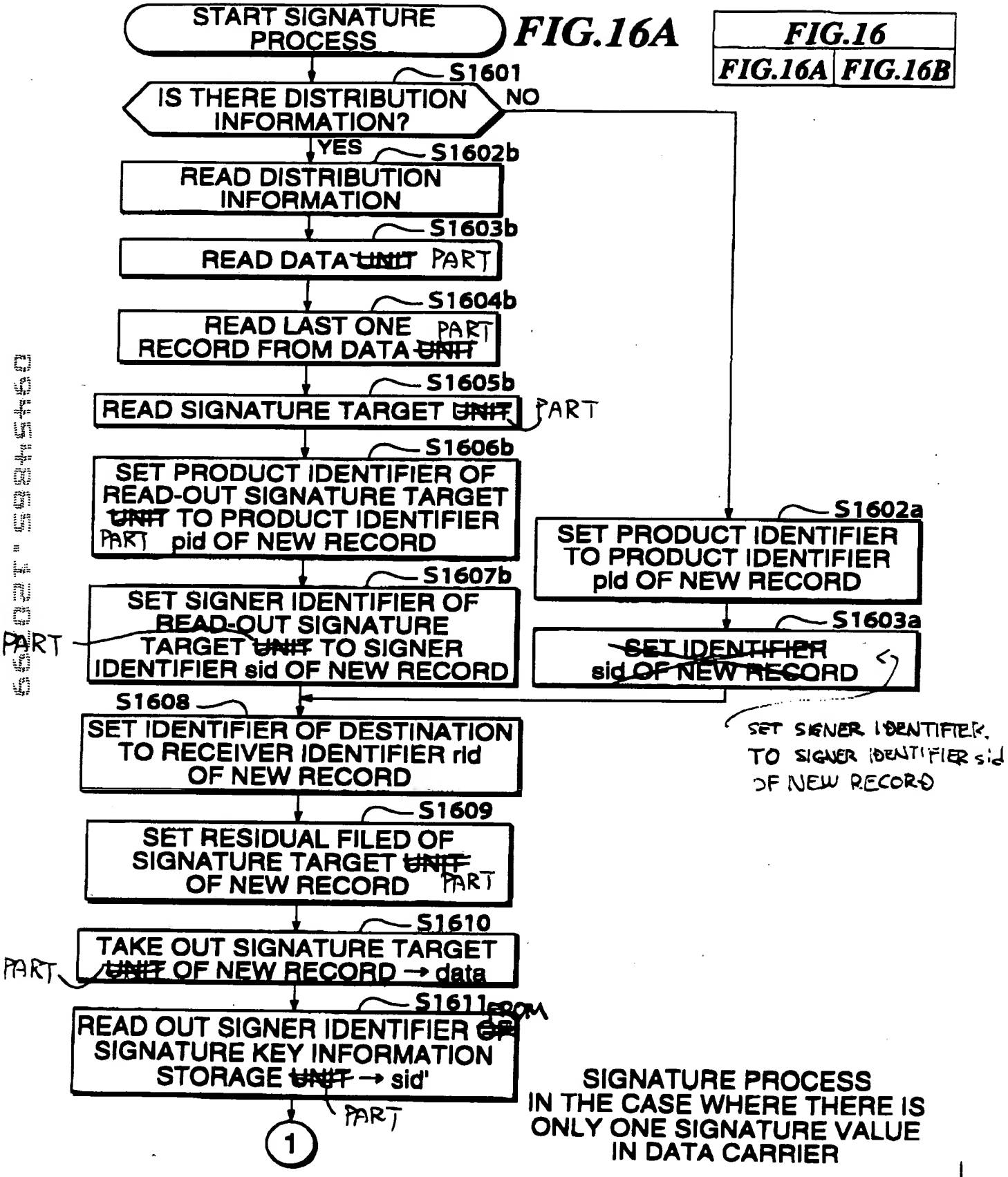


SIGNATURE VERIFICATION PROCESSIN THE CASE WHERE THERE IS ONLY ONE SIGNATURE VALUE IN DATA CARRIER

FIG.16

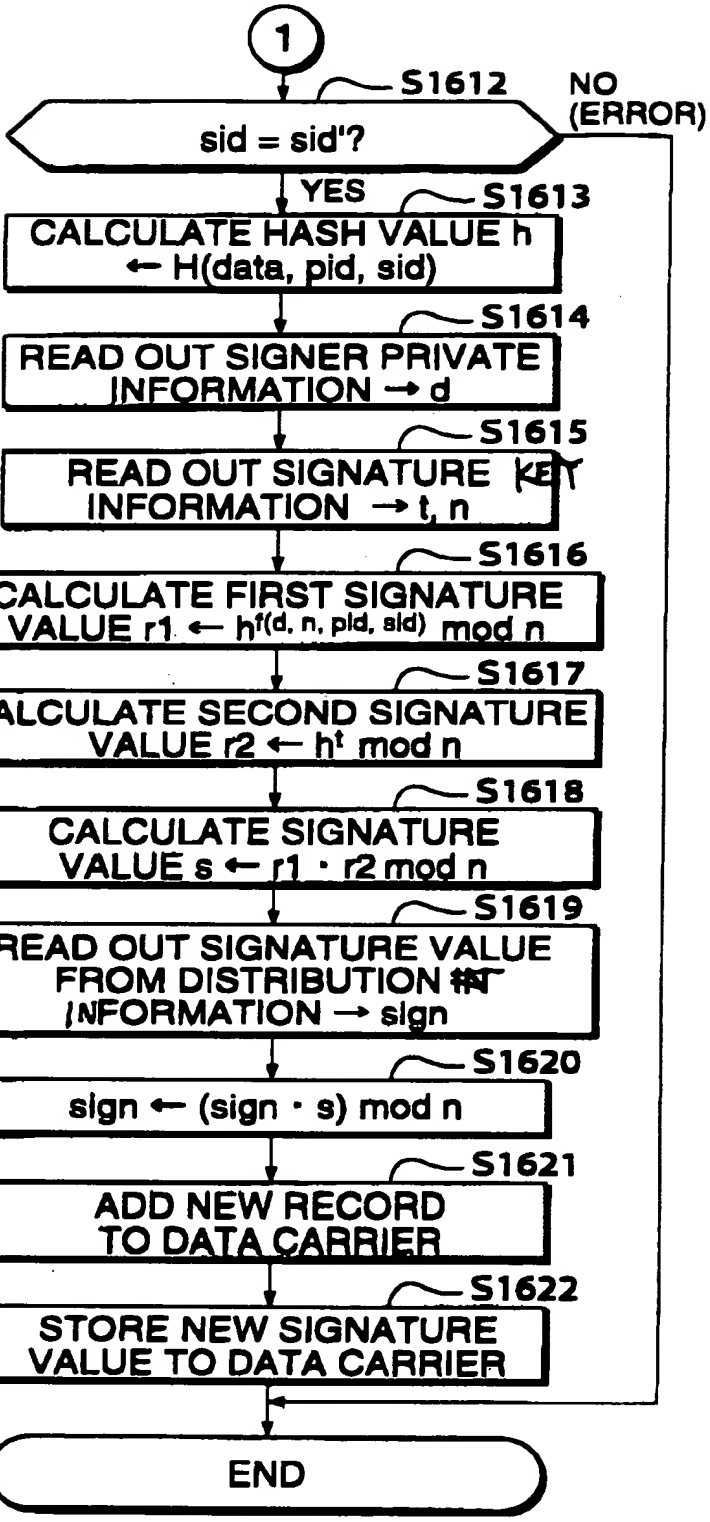
FIG.16A	FIG.16B

FIG.16A



SIGNATURE PROCESS IN THE CASE WHERE THERE IS ONLY ONE SIGNATURE VALUE IN DATA CARRIER

FIG.16B



SIGNATURE PROCESS IN THE CASE WHERE THERE IS ONLY ONE SIGNATURE VALUE IN DATA CARRIER

FIG.17A

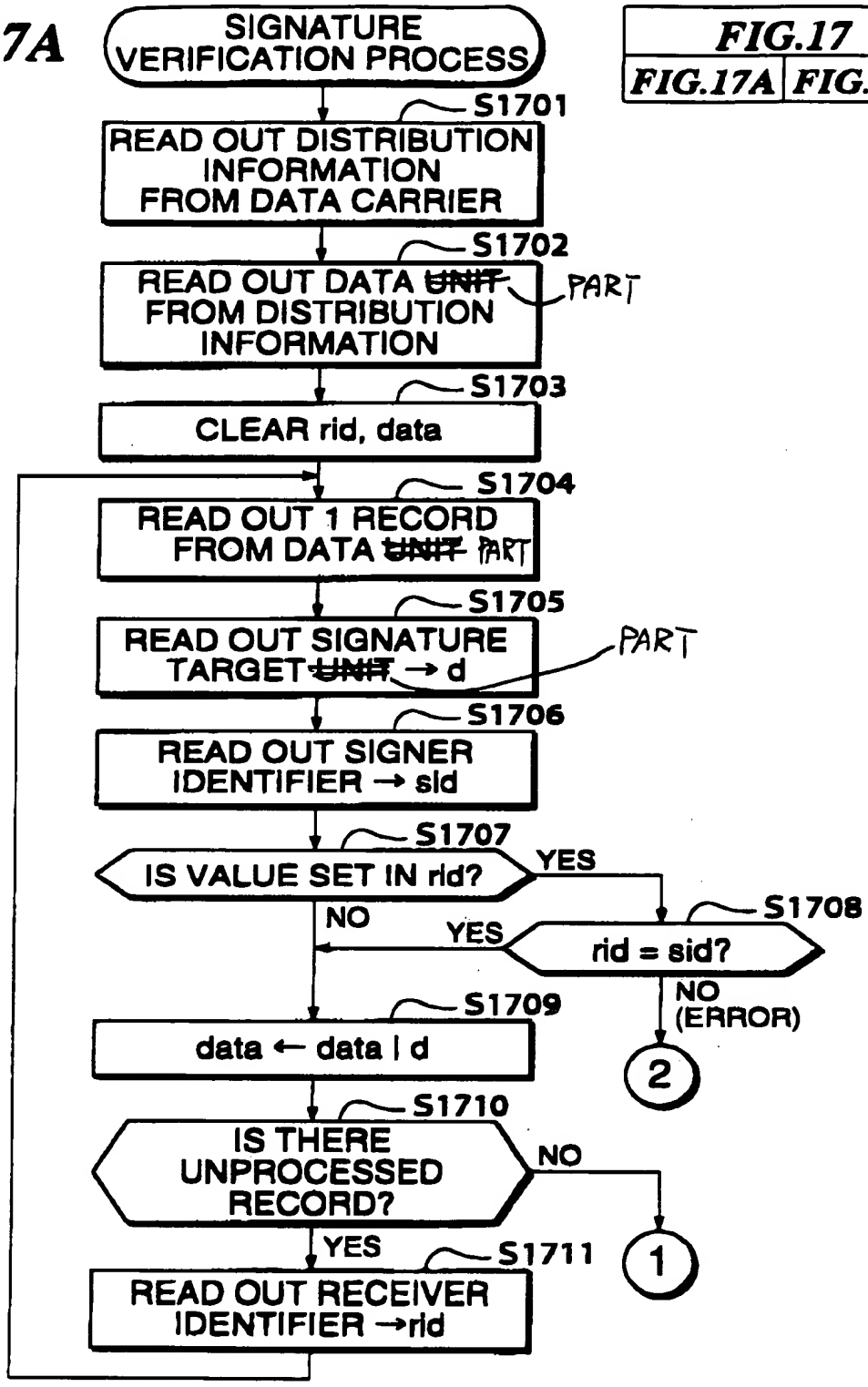
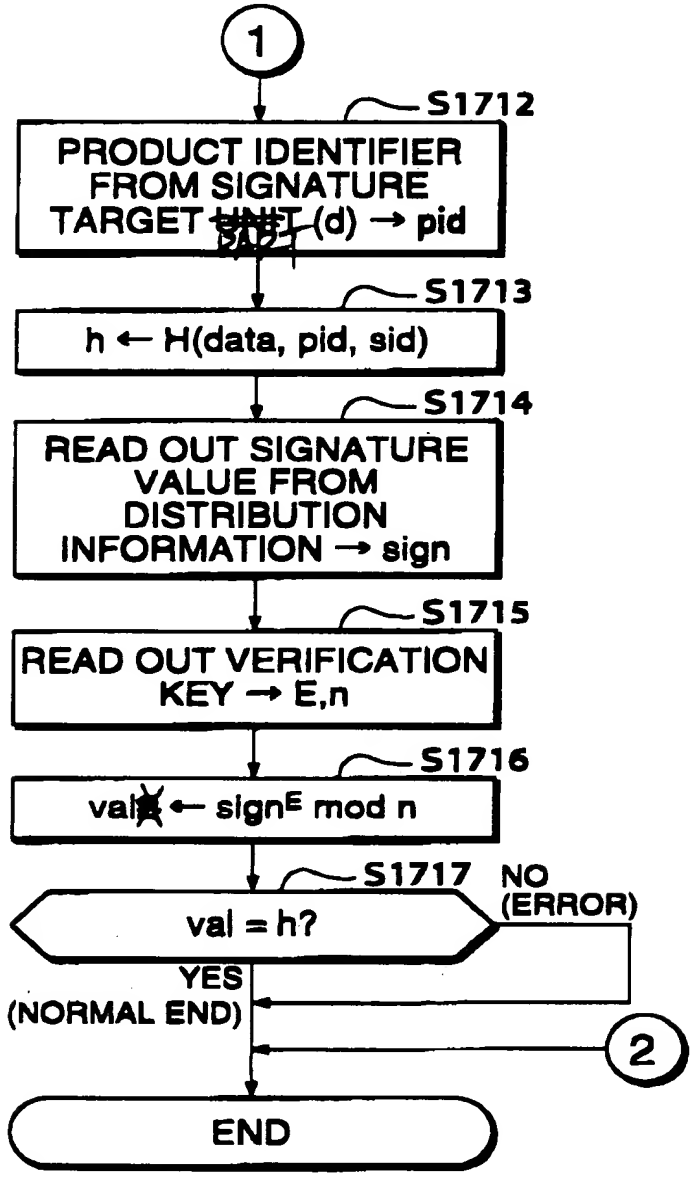


FIG.17

FIG.17A	FIG.17B

VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (ONE VERIFICATION KEY)

FIG.17B



VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (ONE VERIFICATION KEY)

FIG.18A

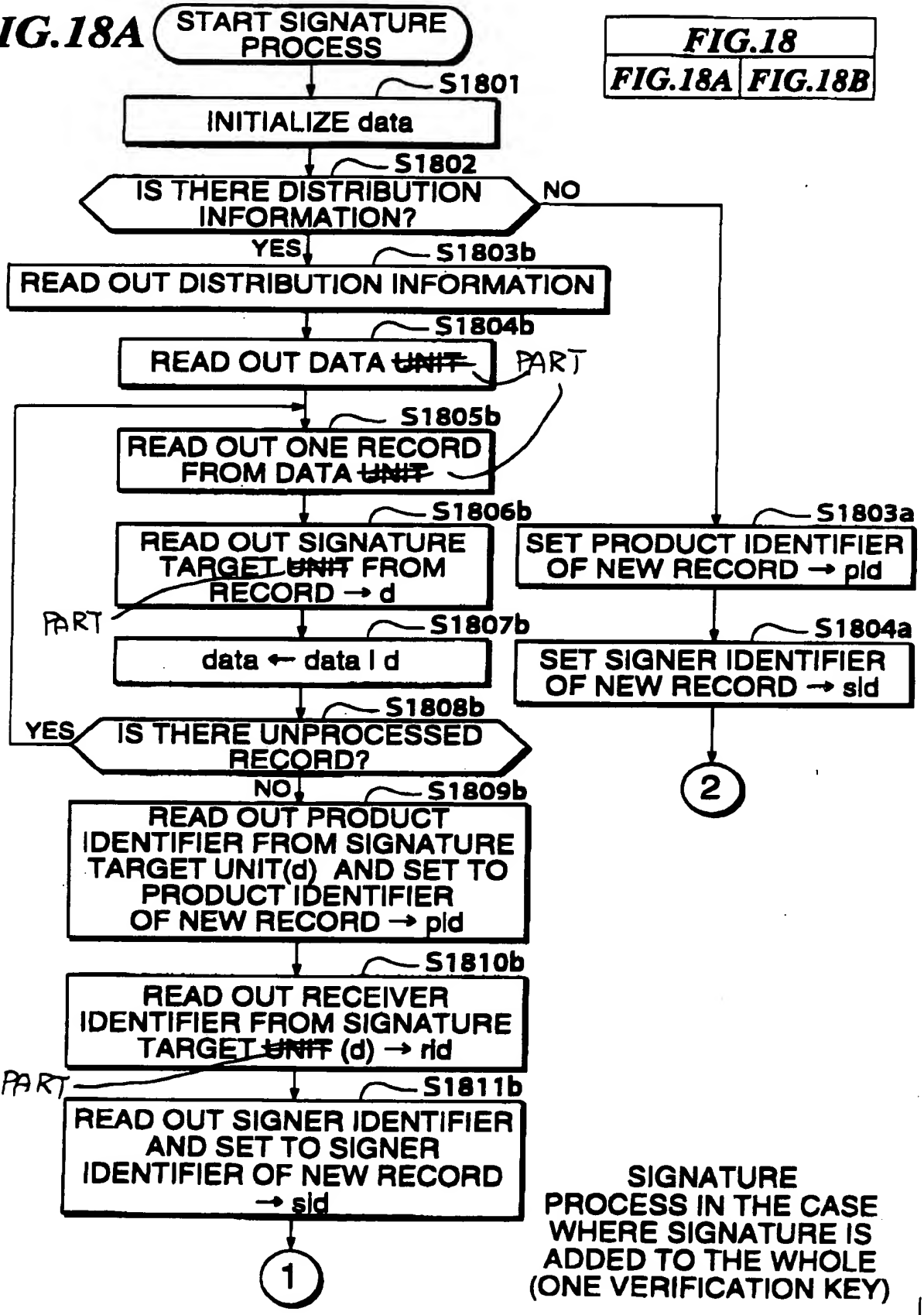
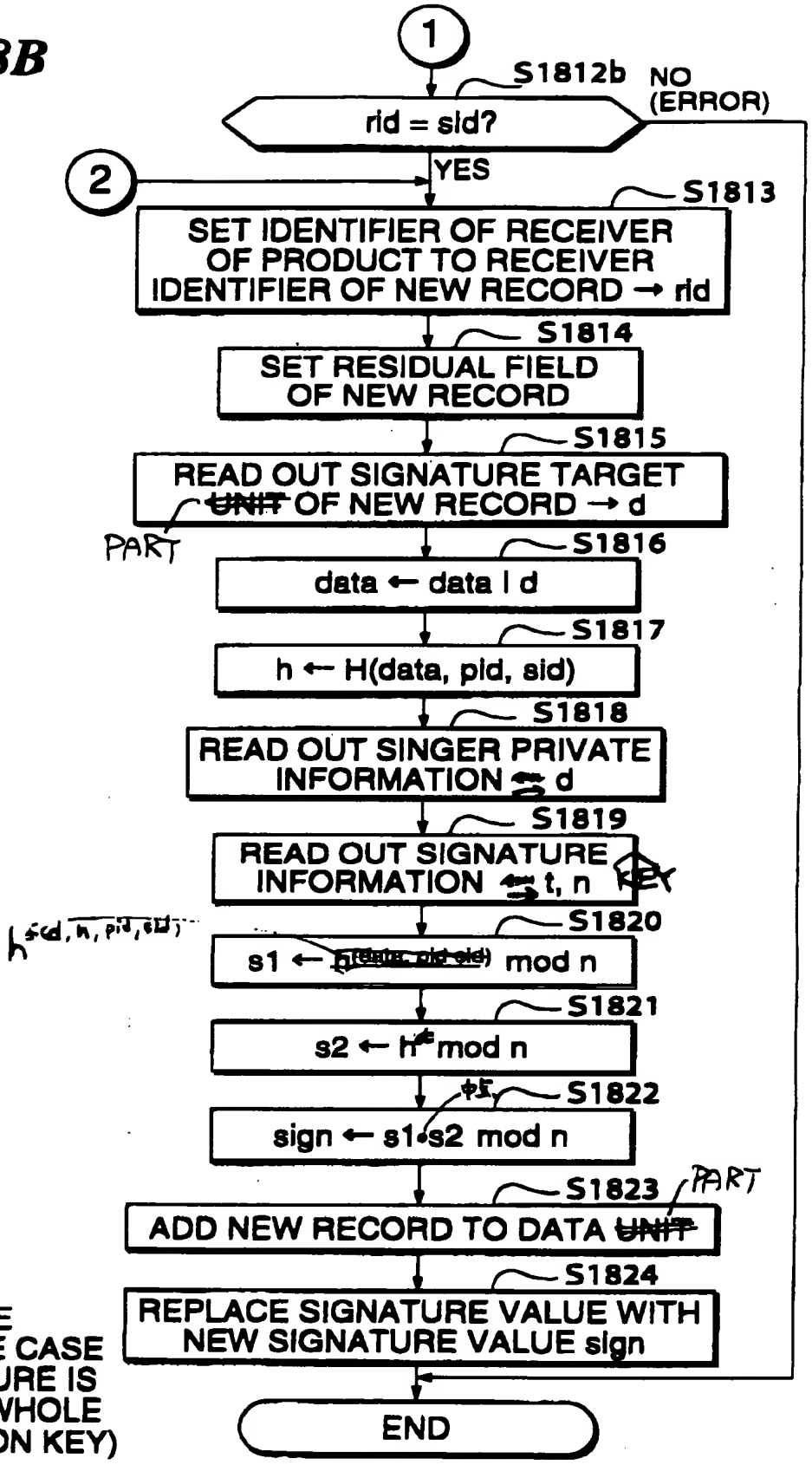


FIG.18
FIG.18A | FIG.18B

SIGNATURE PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (ONE VERIFICATION KEY)

FIG.18B



SIGNATURE PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (ONE VERIFICATION KEY)

FIG.19

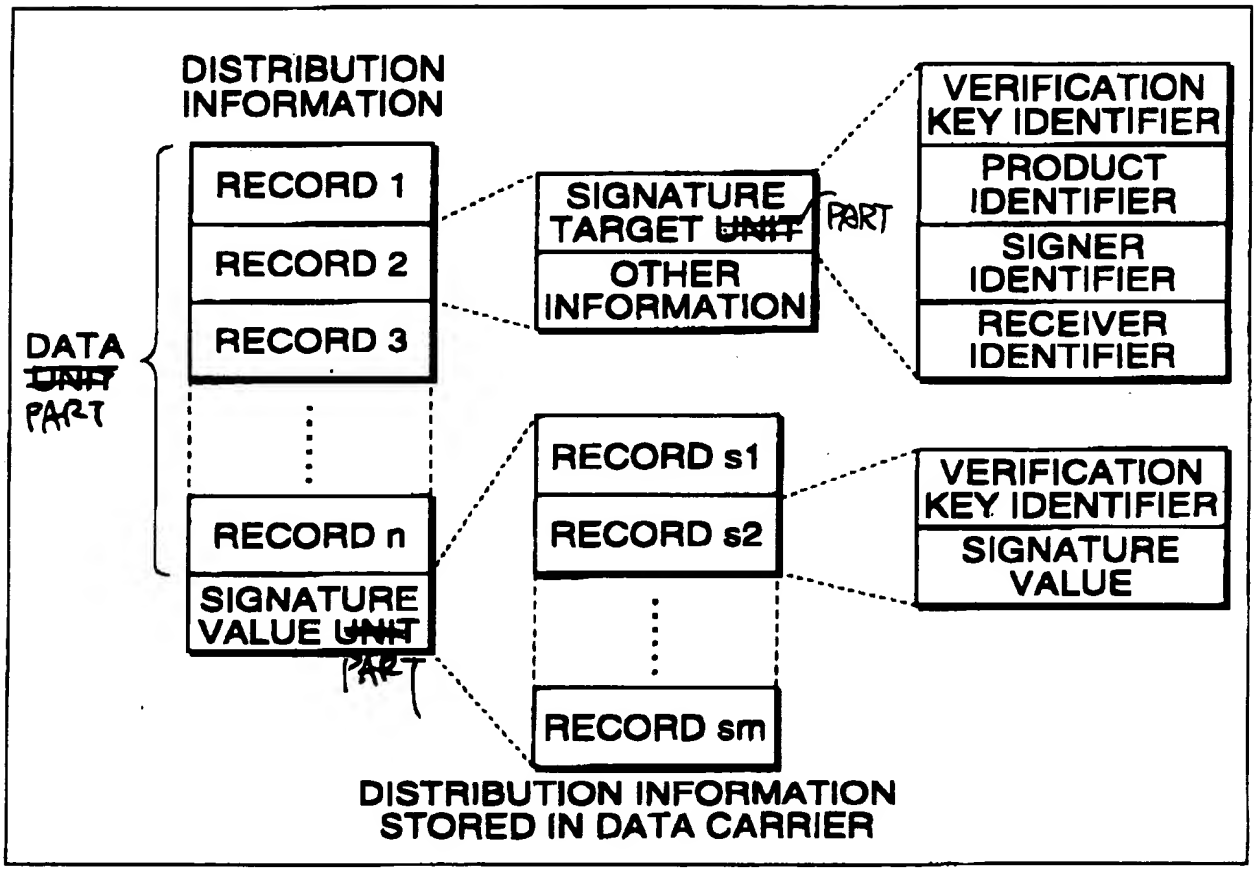

DISTRIBUTION INFORMATION
RECORD 1
RECORD 2
RECORD 3
RECORD n
SIGNATURE VALUE UNIT
DATA UNIT PART
SIGNATURE TARGET UNIT
OTHER INFORMATION
PART
VERIFICATION KEY IDENTIFIER
PRODUCT IDENTIFIER
SIGNER IDENTIFIER
RECEIVER IDENTIFIER
RECORD s1
RECORD s2
RECORD sm
VERIFICATION KEY IDENTIFIER
SIGNATURE VALUE
DISTRIBUTION INFORMATION STORED IN DATA CARRIER

FIG.20

FIG.20A	FIG.20B

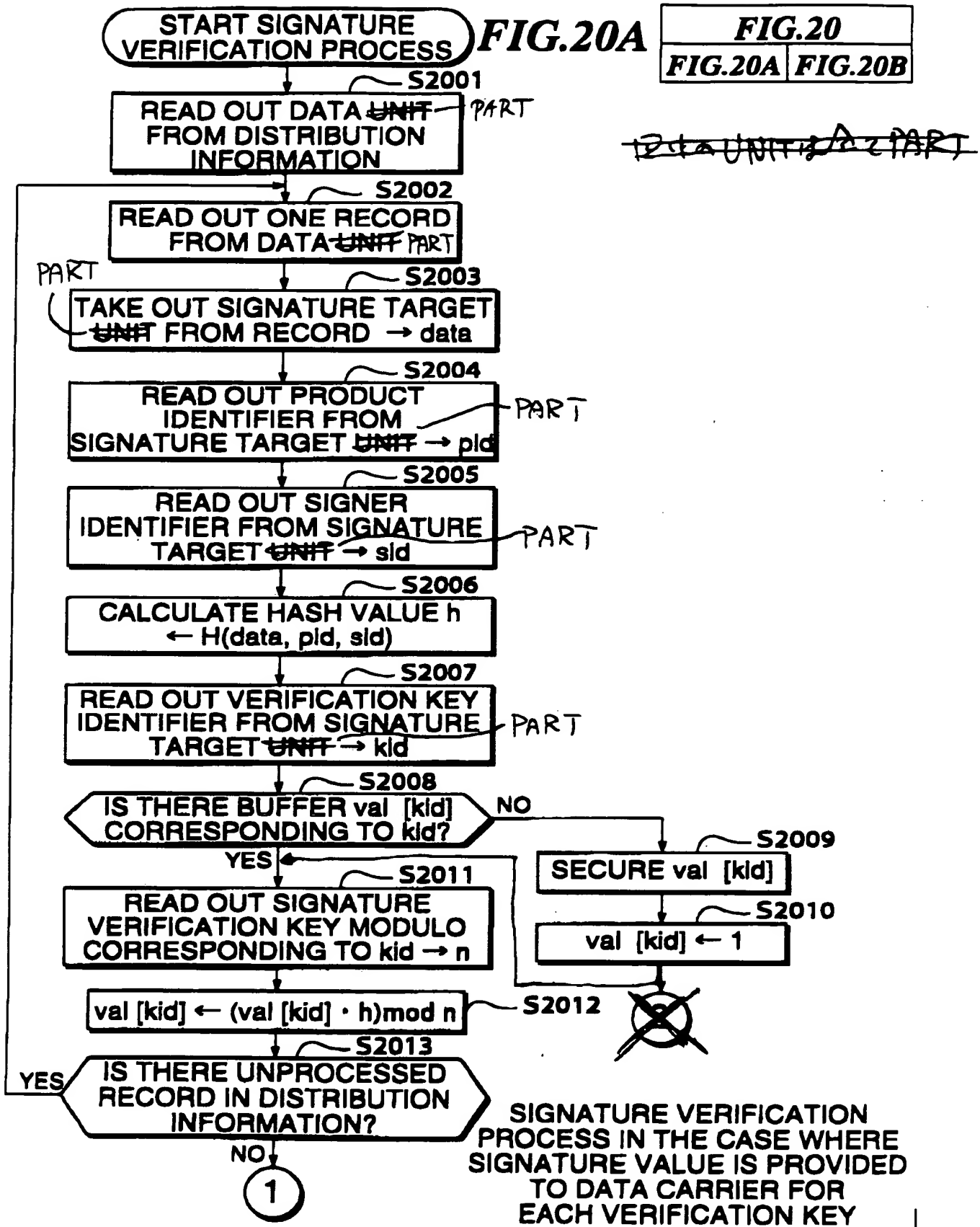
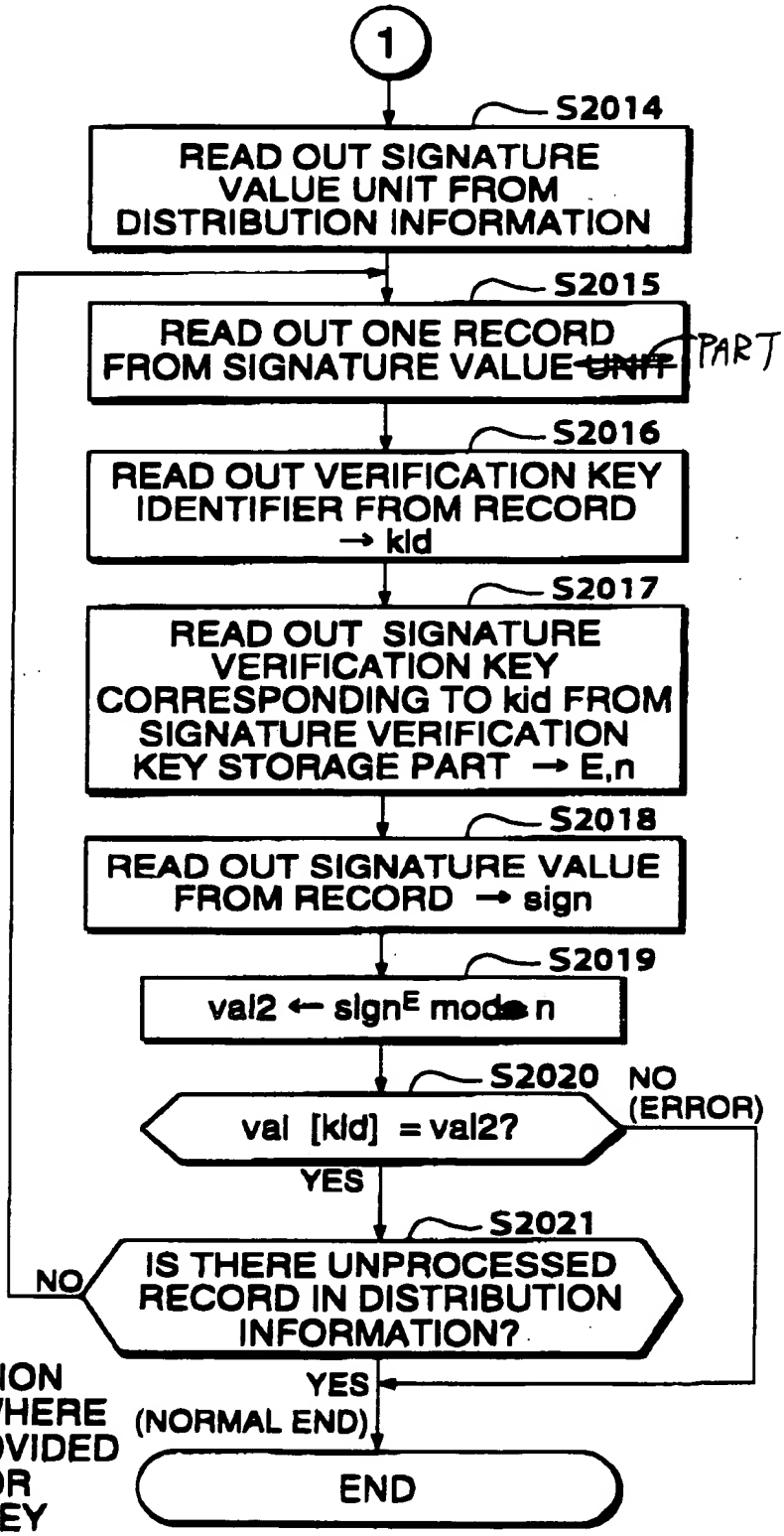


FIG.20A

SIGNATURE VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE VALUE IS PROVIDED TO DATA CARRIER FOR EACH VERIFICATION KEY

FIG.20B



SIGNATURE VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE VALUE IS PROVIDED TO DATA CARRIER FOR EACH VERIFICATION KEY

FIG.21A

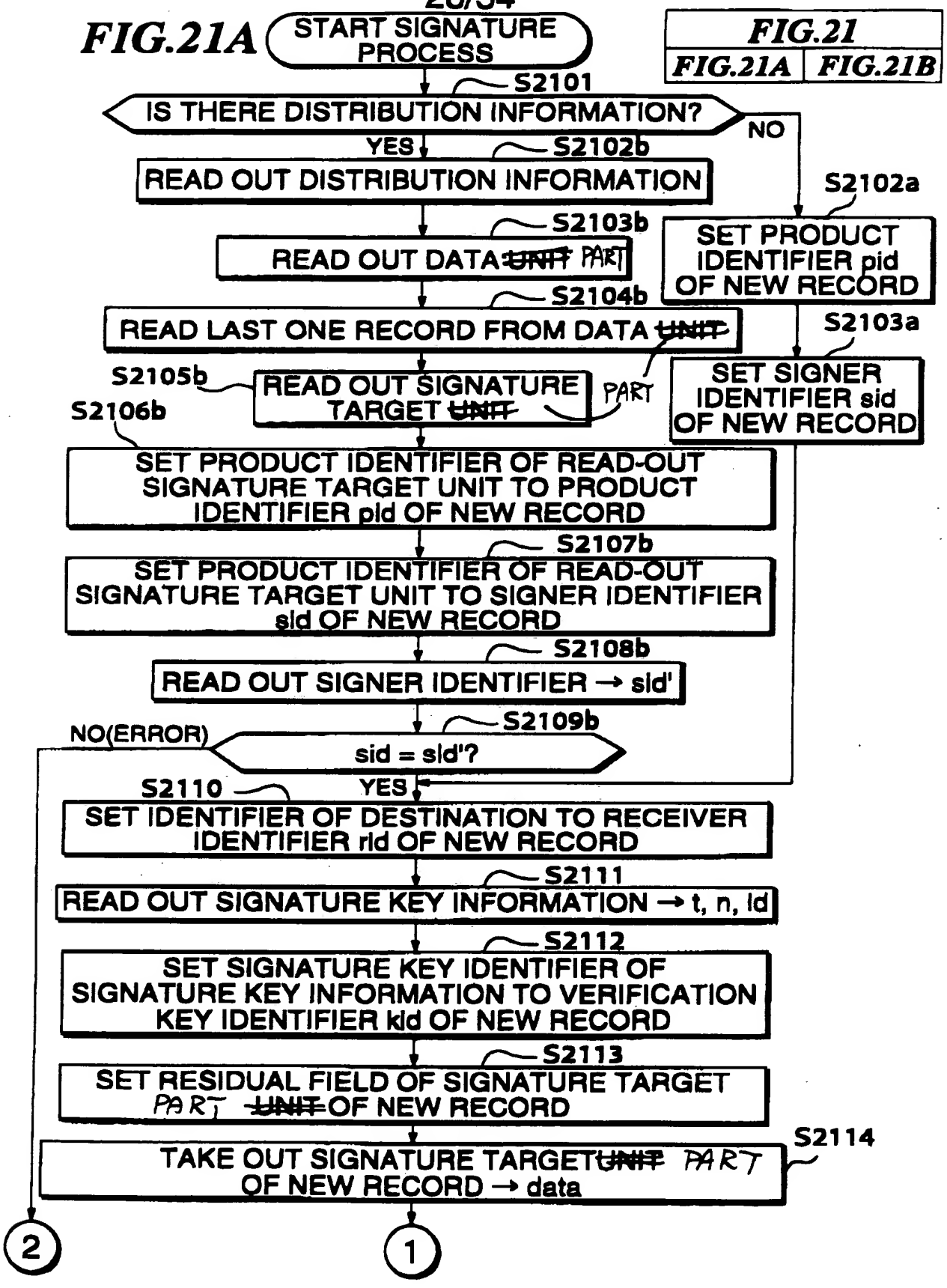
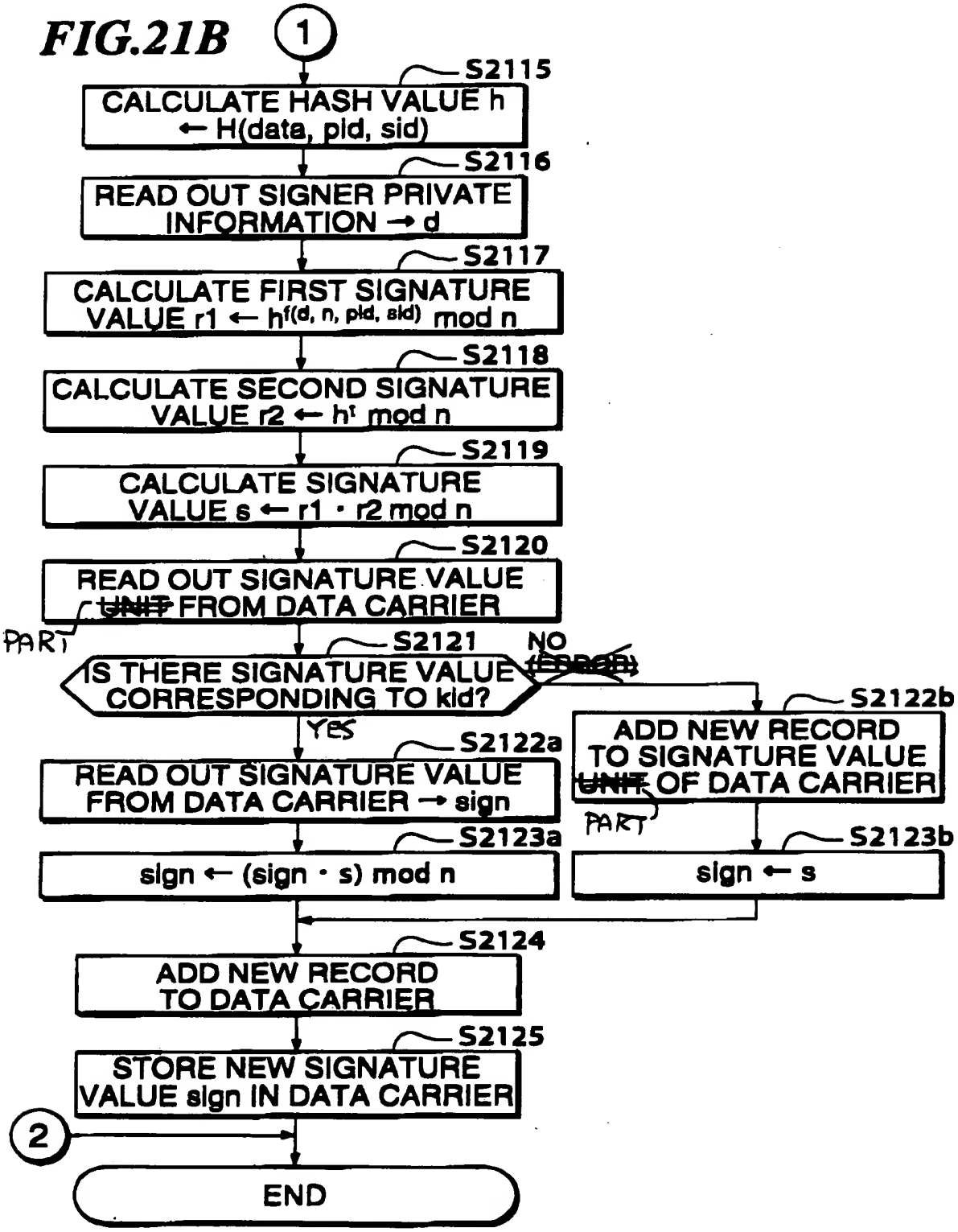


FIG.21

FIG.21A	FIG.21B

FIG.21B



SIGNATURE PROCESS IN THE CASE WHERE SIGNATURE VALUE IS PROVIDED IN DATA CARRIER FOR EACH VERIFICATION KEY

FIG.22A

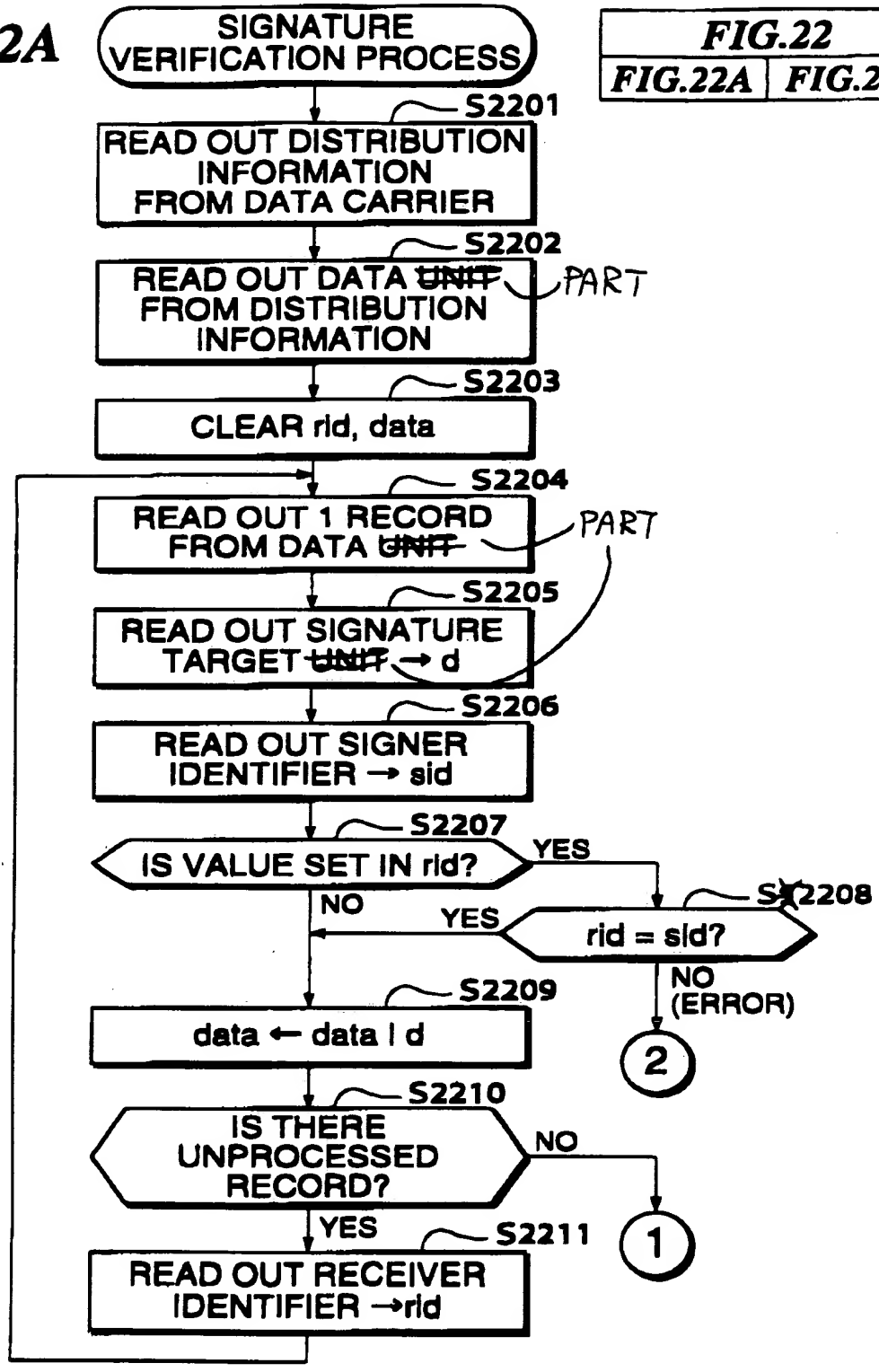


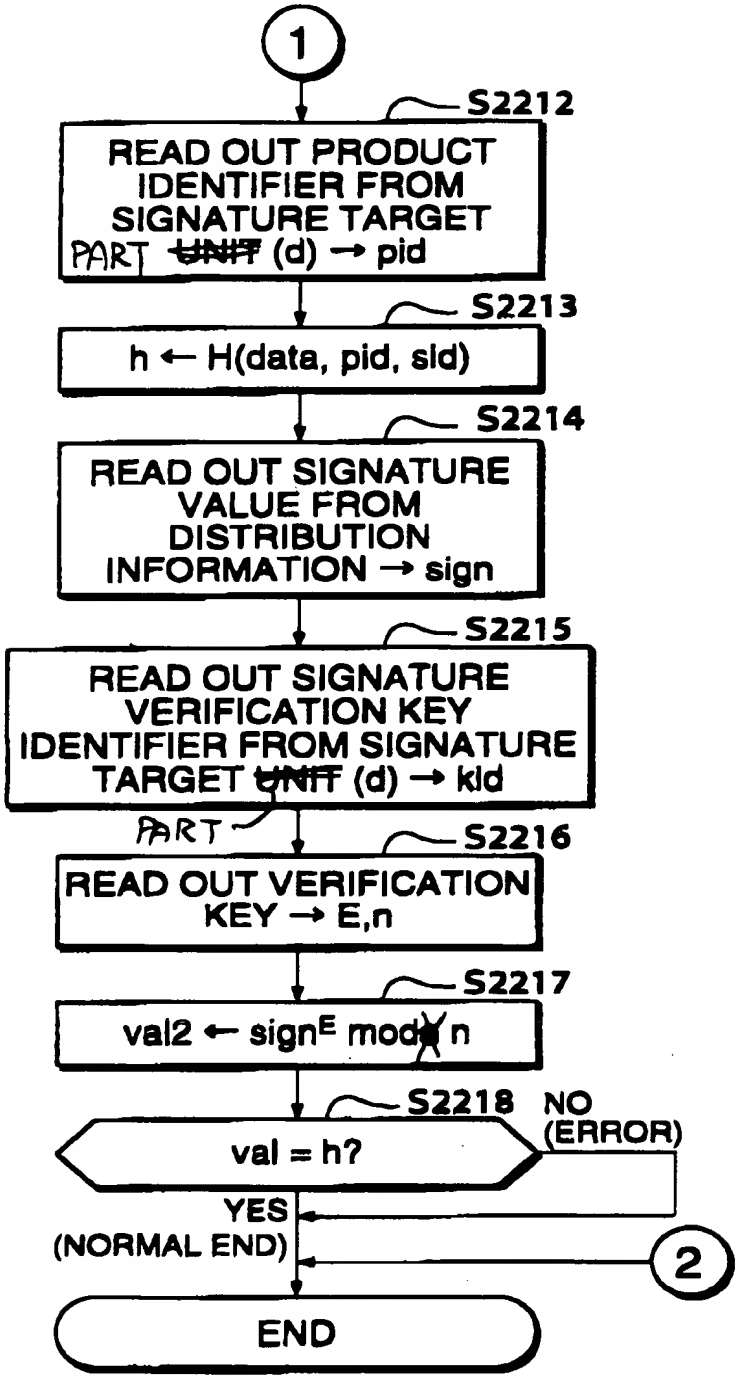
FIG.22

FIG.22A	FIG.22B

VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (~~A PLURALITY OF~~ VERIFICATION KEYS)

PLURAL

FIG.22B



VERIFICATION PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (~~A PLURALITY OF~~ VERIFICATION KEYS)

PLURAL

FIG.23A

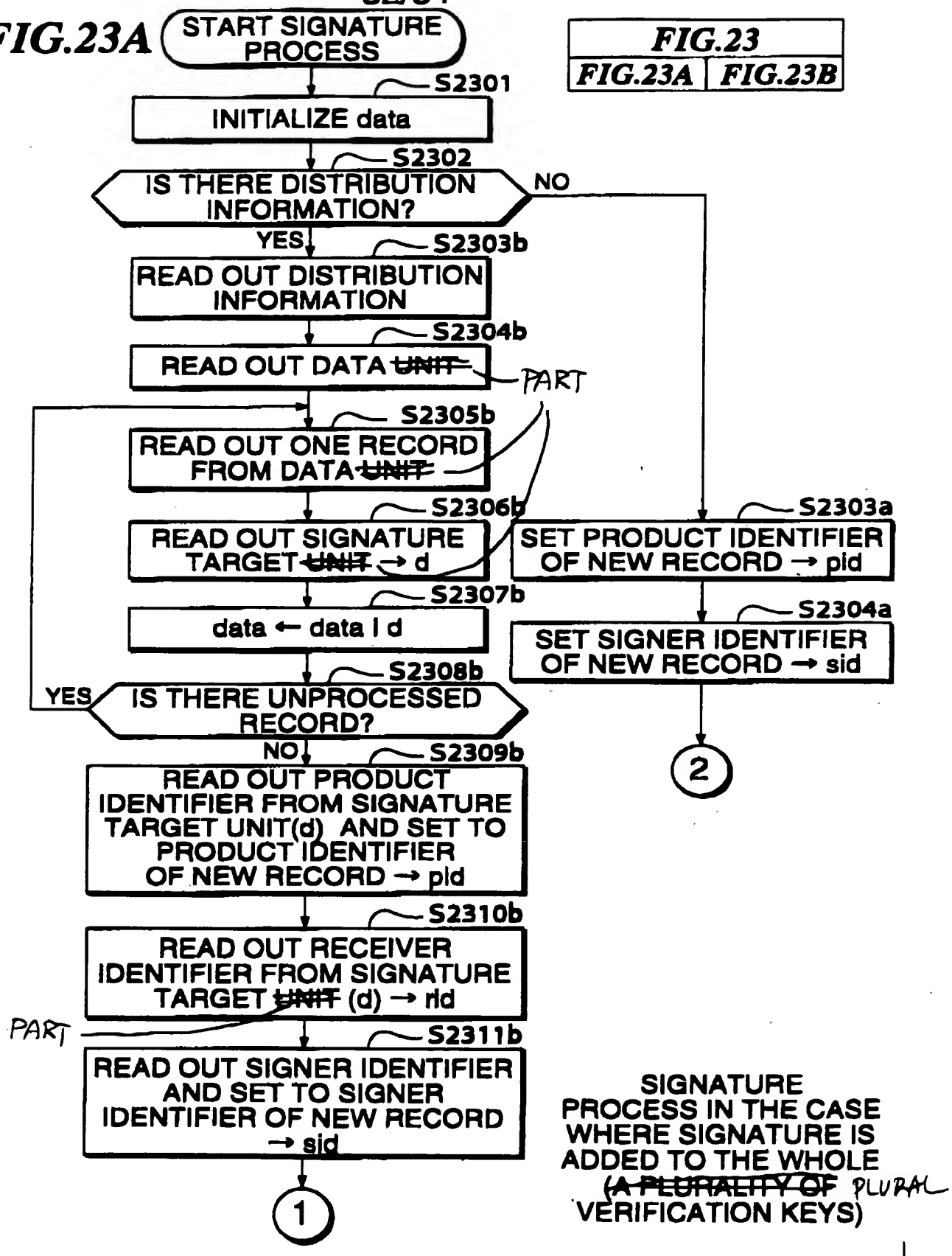
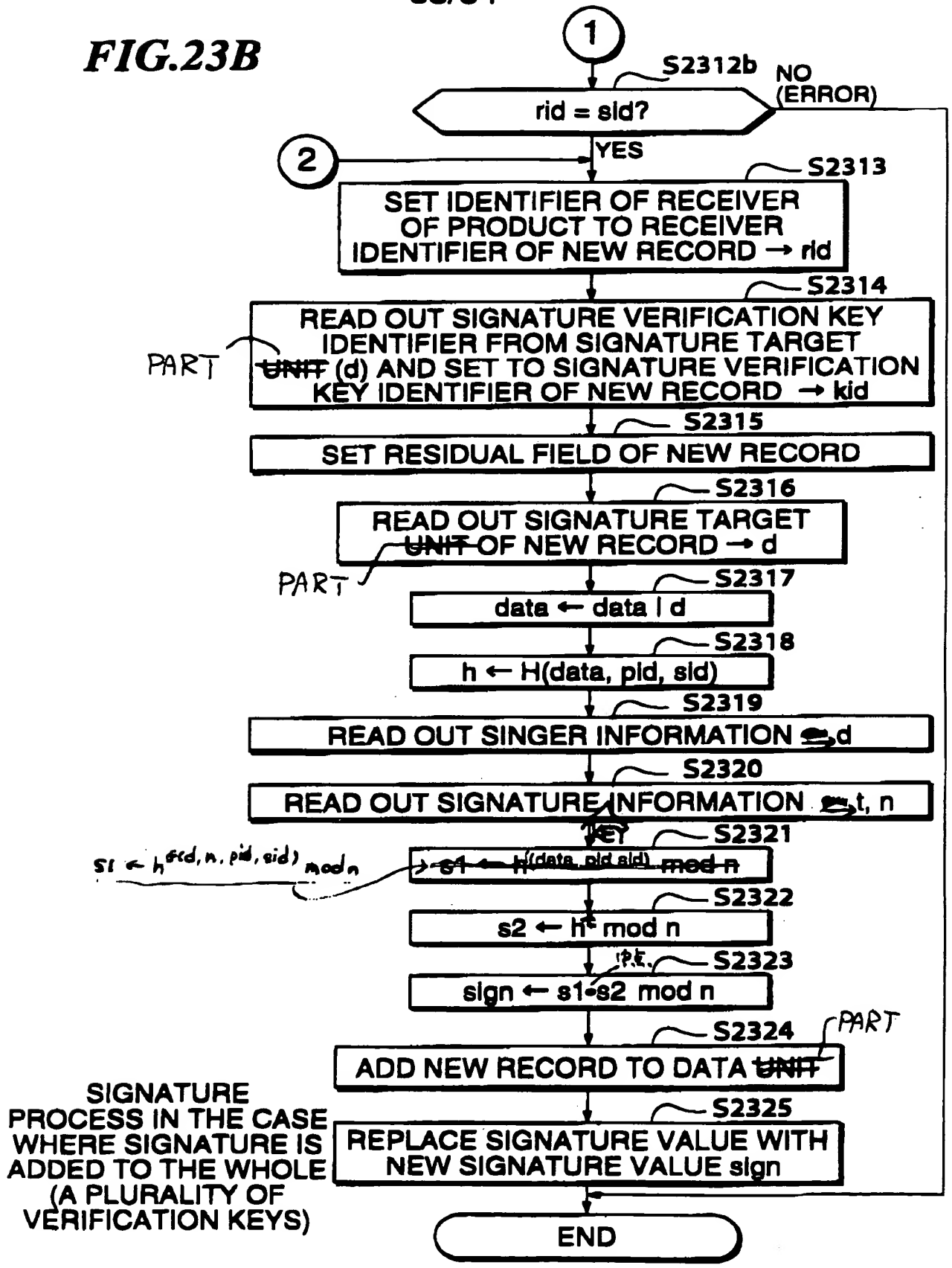


FIG.23

FIG.23A	FIG.23B

SIGNATURE PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (~~A PLURALITY OF~~ PLURAL VERIFICATION KEYS)

FIG.23B



SIGNATURE PROCESS IN THE CASE WHERE SIGNATURE IS ADDED TO THE WHOLE (A PLURALITY OF VERIFICATION KEYS)